Exhibit 9

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Gregory G. Raleigh	Attorney Docket No. 39843-0185IP1
U.S. Patent No.:	11,405,429	
Issue Date:	August 2, 2022	
Appl. Serial No.:	16/907,887	
Filing Date:	June 22, 2020	
Title:	SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES	

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 11,405,429 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

EXHIBITS

SAMSUNG-1001	U.S. Patent No. 11,405,429 to Gregory G. Raleigh ("the '429 Patent")
SAMSUNG-1002	Excerpts from the Prosecution History of the '429 Patent ("the Prosecution History")
SAMSUNG-1003	Declaration and Curriculum Vitae of Dr. Patrick McDaniel.
SAMSUNG-1004	Complaint, *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al,* 2-24-cv-00228, E.D. Tex., filed April 3, 2024
SAMSUNG-1005	U.S. Pat. App. Pub. No. 2009/0077643 ("Schmidt")
SAMSUNG-1006	U.S. Pat. App. Pub. No. 2005/0101323 ("De Beer")
SAMSUNG-1007	U.S. Pat. App. Pub. No. 2004/0148237 ("Bittmann")
SAMSUNG-1008	(Excerpts) Smith, et al., 2005. "Virtual Machines: Versatile Platforms for Systems and Processes," Elsevier, Inc, 2005, ISBN 1-55860-910-5 ("Smith")
SAMSUNG-1009	Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings, June 21, 2022, available at https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf
SAMSUNG-1010	Samsung Stipulation Letter
SAMSUNG-1011	Docket Control Order, CASE NO. 2:24-CV-00228-JRG-RSP
SAMSUNG-1012	Declaration of June Munford
SAMSUNG-1013-1019	RESERVED
SAMSUNG-1020	U.S. Pat. App. Pub. No. 2009/0149165 ("Minborg")

SAMSUNG-1021	U.S. Pat. App. Pub. No. 2007/0117538 ("Weiser")
SAMSUNG-1022	(Excerpts) Telecom Dictionary, Athos Publishing, 2007.
SAMSUNG-1023	(Excerpts) Eberspächer, Jörg (2001). GSM Switching, Services and Protocols, Second Edition. John Wiley & Sons Ltd. ISBN: 978-0-470-85394-8.
SAMSUNG-1024	RESERVED
SAMSUNG-1025	3rd Generation Partnership Project; Technical Specification Group Terminals; "Characteristics of the USIM application" (Release 7), 3GPP TS 31.102 V7.0.0 ("3GPP USIM").
SAMSUNG-1026	U.S. Pat. No. 5,764,693 ("Taylor")
SAMSUNG-1027	U.S. Pat. No. 6,470,182 ("Nelson")
SAMSUNG-1028	U.S. Pat. App. Pub. No. 2006/0015749 ("Mittal")
SAMSUNG-1029	Kasper, et al., 2008, February. "Subscriber authentication in cellular networks with trusted virtual sims." In 2008 10th International Conference on Advanced Communication Technology (Vol. 2, pp. 903-908). IEEE. ("Kasper")
SAMSUNG-1030	TCG Mobile Reference Architecture, version 1.0, Revision 1, June 12, 2007. ("TCG Mobile Reference Architecture")
SAMSUNG-1031	TCG Mobile Trusted Module Specification, version 1.0, Revision 6, June 26, 2008. ("TCG Mobile Trusted Module Specification")
SAMSUNG-1032	U.S. Pat. App. Pub. No. 2006/0020781A1 ("Scarlata")
SAMSUNG-1033	U.S. Pat. No. 6,421,722 ("Bauer")
SAMSUNG-1034	U.S. Pat. App. Pub. No. 2007/0178888 ("Alfano")
SAMSUNG-1035	U.S. Pat. App. Pub. No. 2008/0117958 ("Pattenden")

SAMSUNG-1036	Stone, G.N., Lundy, B. and Xie, G.G., 2001. Network policy languages: a survey and a new approach. IEEE network, 15(1), pp.10-21. ("Stone")
SAMSUNG-1037	U.S. Pat. No. 6,556,823 ("Clapton")
SAMSUNG-1038	U.S. Pat. App. Pub. No. 2007/0149252 ("Jobs")
SAMSUNG-1039	RESERVED
SAMSUNG-1040	David K. Gifford. 1982. Cryptographic sealing for information secrecy and authentication. Commun. ACM 25, 4 (April 1982), 274–286. https://doi.org/10.1145/358468.358493
SAMSUNG-1041	RESERVED
SAMSUNG-1042	Jansen, Wayne A. and Richard P. Ayers. "Forensic Tools for Mobile Phone Subscriber Identity Modules." J. Digit. Forensics Secur. Law 1 (2006): 75-94.
SAMSUNG-1043-1048	RESERVED
SAMSUNG-1049	National Institute of Standards and Technology. 2001. Security Requirements for Cryptographic Modules, downloaded from the Internet at https://nvl-pubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf on December 5, 2024
SAMSUNG-1050	Verma, et. al., (2002). Policy-based management of content distribution networks. IEEE network, 16(2), 34-39. ("Verma")
SAMSUNG-1051	Lobo, et. al., (1999). A policy description language. AAAI/IAAI, 1999, 291-298. ("Lobo")
SAMSUNG-1052	Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, November 2001, downloaded from the Internet on May 27, 2024.
SAMSUNG-1053	RESERVED

SAMSUNG-1054	(Excerpts) Keith Mayes and Konstantinos Markantonakis. 2008. Smart Cards, Tokens, Security and Applications (1st. ed.). ("Mayes")
SAMSUNG-1055	(Excerpts) Gasser, Morrie. Building a Secure Computer System. New York, NY: Van Nostrand Reinhold, 1988. ("Gasser")
SAMSUNG-1056	(Excerpts) Malhotra, Ravi. 2002. IP Routing: Help for Network Administrators. O'Reilly Media. ISBN: 978-0-596-00275-0 ("Malhotra")
SAMSUNG-1057	Jude, Michael. "Policy-Based Management: Beyond the Hype." Business Communications Review 31.3 (2001): 52-56. ("Jude")
SAMSUNG-1058	Merkle, Ralph C. 1978. Secure communications over insecure channels. Commun. ACM 21, 4 (April 1978), 294–299. https://doi.org/10.1145/359460.359473 ("Merkle")
SAMSUNG-1059	ARM. 2004. PrimeCell Infrastructure AMBA 3 TrustZone Protection Controller (BP147) Revision: r0p0 Technical Overview, downloaded from the Internet at https://documentation-service.arm.com/static/5e9565afc8052b1608762aae%3Ftoken%3D&ved=2ahUKEwiZq56_3pGKAxVUCnkGHcR9OGIQFnoECAwQAQ&usg=AOvVaw2PG8jUG9TU8fpiRxmGKNyM on December 5, 2024
SAMSUNG-1060	Network Associates, Inc. 1999. PGP, Version 6.5.1. An Introduction to Cryptography.
SAMSUNG-1061	Stuart E. Madnick and John J. Donovan. 1973. Application and analysis of the virtual machine approach to information system security and isolation. In Proceedings of the workshop on virtual computer systems. Association for Computing Machinery, New York, NY, USA, 210–224. https://doi.org/10.1145/800122.803961

SAMSUNG-1062	U.S. Pat. App. Pub. No. 2008/0122796 (“Jobs-796”)
SAMSUNG-1063	European Telecommunications Standards Institute. 1998. Terrestrial Trunked Radio (TETRA); Security Aspects; Subscriber Identity Module to Mobile Equipment (SIM – ME) interface. ETSI ETS 300 812 ed.1 (1998-11), downloaded from the Internet at https://www.etsi.org/deliver/etsi_i_ets/300800_300899/300812/01_20_9826/ets_300812e01c.pdf on December 12, 2024
SAMSUNG-1064	IETF RFC 1122, Requirements for Internet Hosts – Communication Layers, October 1989, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc1122 on December 12, 2024.
SAMSUNG-1065	IETF RFC 793, Transmission Control Protocol, September 1981, downloaded from the internet at https://www.ietf.org/rfc/rfc793.txt on December 11, 2024.
SAMSUNG-1066	U.S. Pat. App. Pub. No. 2005/0108534 (“Bajikar”)
SAMSUNG-1067	Smith, et al., 2005. “The architecture of virtual machines. Computer,” 38(5) (“Smith-2005”)
SAMSUNG-1068	ISO/IEC 7498-1, “Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model,” downloaded from the internet at https://www.ecma-international.org/wp-content/uploads/s020269e.pdf on January 10, 2025 (“OSI”)
SAMSUNG-1069	Gonçalves, et al., 2009, October. A graphical user interface for policy composition in CIM-SPL. In 2009 International Conference on Ultra Modern Telecommunications & Workshops (pp. 1-7). IEEE. (“Gonçalves”)
SAMSUNG-1070	Agrawal, et. al., 2007, May. Issues in designing a policy language for distributed management of IT infrastructures. In 2007 10th IFIP/IEEE International Symposium on Integrated Network Management (pp. 30-39). IEEE. (“Agrawal-2”)

CLAIMS

Claim	Identifier	Claim Language
1	[1.1]	A method of operating a wireless end-user device, the method comprising:
	[1.2]	connecting from a secure modem subsystem to a wireless cellular network;
	[1.3]	connecting a first secure control channel from the secure modem subsystem through the wireless cellular network to a network service controller;
	[1.4]	connecting a second secure control channel from a secure execution environment, separately secure from the secure modem subsystem, through the secure modem subsystem and the wireless cellular network to the network service controller;
	[1.5]	receiving at the secure execution environment, via the second secure control channel, one or more messages from the network service controller, the one or more messages comprising one or more service policy settings;
	[1.6]	storing the one or more service policy settings in a secure memory partition accessible only from the secure execution environment; and
	[1.7]	enforcing, at least in part from the secure execution environment, a network service profile comprising the one or more service policy settings, to control the wireless end-user device use of a service on the wireless cellular network.
2	[2]	The method of claim 1, wherein the network service profile is associated with a service plan that provides for access to the service on the wireless cellular network.

3	[3.1]	The method of claim 1, wherein the secure modem subsystem comprises a modem control link and a modem local channel, and the first secure control channel connects the modem control link to the network service controller through the modem local channel, and
	[3.2]	wherein the secure execution environment comprises a host service control link, the second secure control channel coupled to the host service control link, the modem local channel providing secure communication between the modem control link and the host service control link.
4	[4]	The method of claim 1, wherein the secure modem subsystem further comprises a modem agent accessible only by the network service controller through the first secure control channel.
5	[5]	The method of claim 4, wherein the modem agent comprises a service measurement point for use of the service.
6	[6]	The method of claim 5, further comprising the modem agent communicating a first report of the use of the service to the network service controller through the first secure control channel.
7	[7]	The method of claim 6, further comprising the secure execution environment separately communicating a second report of the monitored use of the service through the second secure control channel.
8	[8]	The method of claim 1, wherein the one or more service policy settings include an access control setting, a traffic control setting, and/or an admission control setting.
9	[9]	The method of claim 1, wherein the one or more service policy settings include a network or device management communication setting.

10	[10]	The method of claim 1, wherein the secure execution environment is implemented at least in part as a hardware partition.
11	[11]	The method of claim 1, wherein the secure execution environment is implemented at least in part as a software partition.
12	[12]	The method of claim 1, wherein the secure execution environment is implemented at least in part in a virtual machine executed on a processor.

Samsung Electronics Co., Ltd. (“Petitioner”/“Samsung”) petitions for *Inter Partes* Review (“IPR”) of claims 1-12 (“Challenged Claims”) of U.S. Patent 11,405,429 (“’429 Patent”).

I. IPR REQUIREMENTS

A. Standing

The ’429 Patent is available for IPR. This petition is being filed within one-year of service of a complaint against Samsung. Samsung is not barred/estopped from requesting IPR.

B. Challenge, Relief Requested

Samsung requests an IPR of the Challenged Claims on the below grounds. SAMSUNG-1003, ¶¶1-305.

Ground	Claim(s)	35 U.S.C. § 102/103
1A	1-3, 8-12	Schmidt-De Beer (DB)
1B	4-7	Schmidt-DB-Bittmann
1C	10-12	Schmidt-DB-Smith

Reference	Filed	Published
Schmidt	7/7/2008	3/19/2009
DB	2/14/2002	5/12/2005
Bittmann	1/29/2003	7/29/2004

Reference	Filed	Published
Smith		2005 (*see* SAMSUNG-1012)

C. Claim Construction

Petitioner submits that no formal claim constructions are necessary because "claim terms need only be construed… to resolve the controversy." *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); SAMSUNG-1003, ¶26. Petitioner reserves the right to respond to construction(s) offered by Patent Owner or adopted by the Board. Petitioner is not conceding that each claim satisfies all statutory requirements, nor waiving arguments/ground that cannot be raised here. Petitioner applies prior art consistent with Patent Owner's infringement allegations in litigation.

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art ("POSITA") relating to the '429 Patent's subject matter as of January 28, 2009[1] would have (1) at least a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in wireless communication network

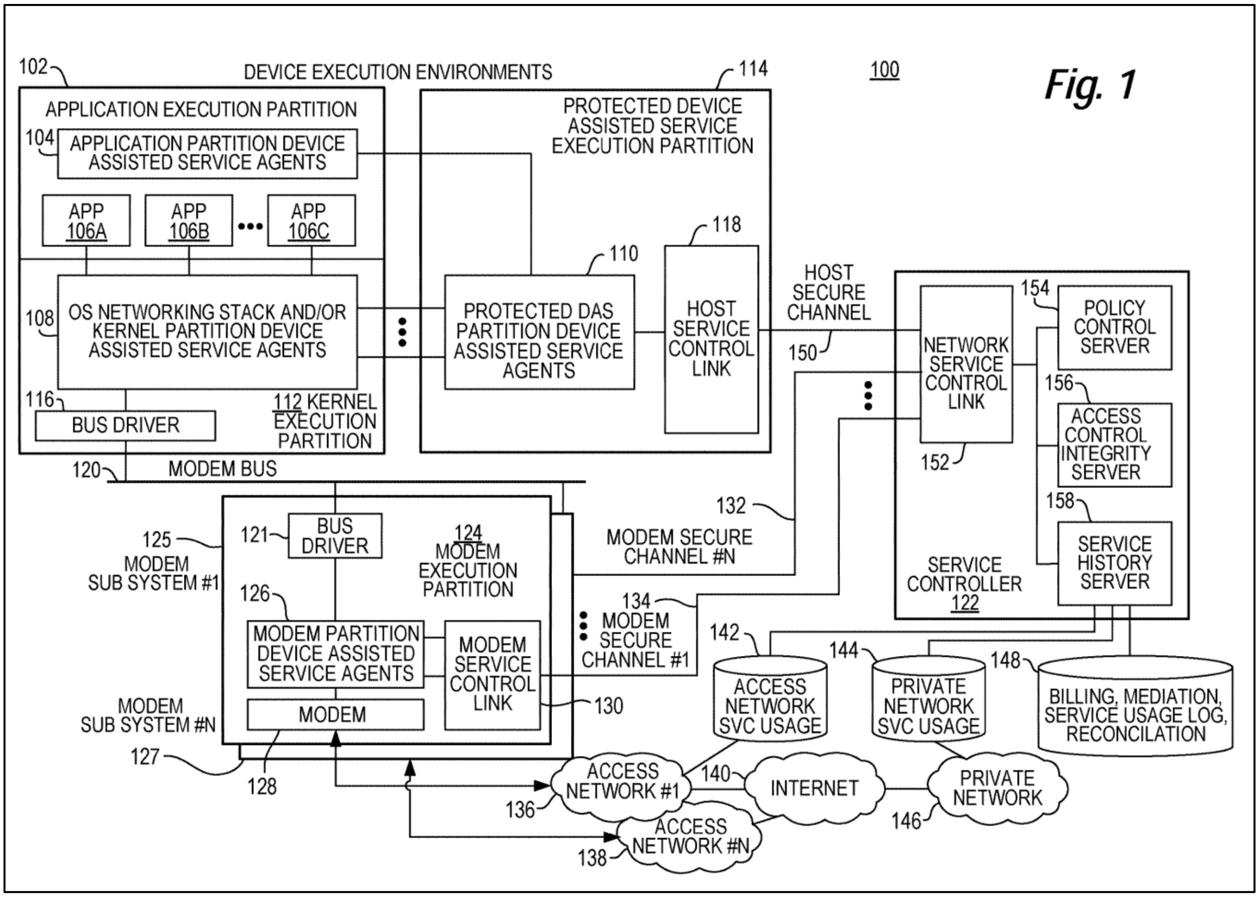
---

[1] Petitioner takes no position regarding whether Challenged Claims are entitled to this priority date.

device applications and software. SAMSUNG-1003, ¶¶24-25. Additional education could substitute for industry experience, and *vice versa*. *Id*. Positions herein and in SAMSUNG-1003 are from the vantage point of a POSITA as of January 28, 2009.

II. THE ’429 PATENT

The ’429 Patent is directed to “security techniques for device assisted services.” SAMSUNG-1001, Abstract. The ’429 patent describes “secure service measurement and/or control execution partition,” “a service profile executed at least in part in a secure execution environment of a processor”, “monitoring use of the service based on the service profile” and verifying service use. *Id.* The application for the ’429 Patent was allowed during prosecution without any art-based rejections. SAMSUNG-1002, 126, 24, 29; SAMSUNG-1003, ¶77.



SAMSUNG-1001, FIG. 1.

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

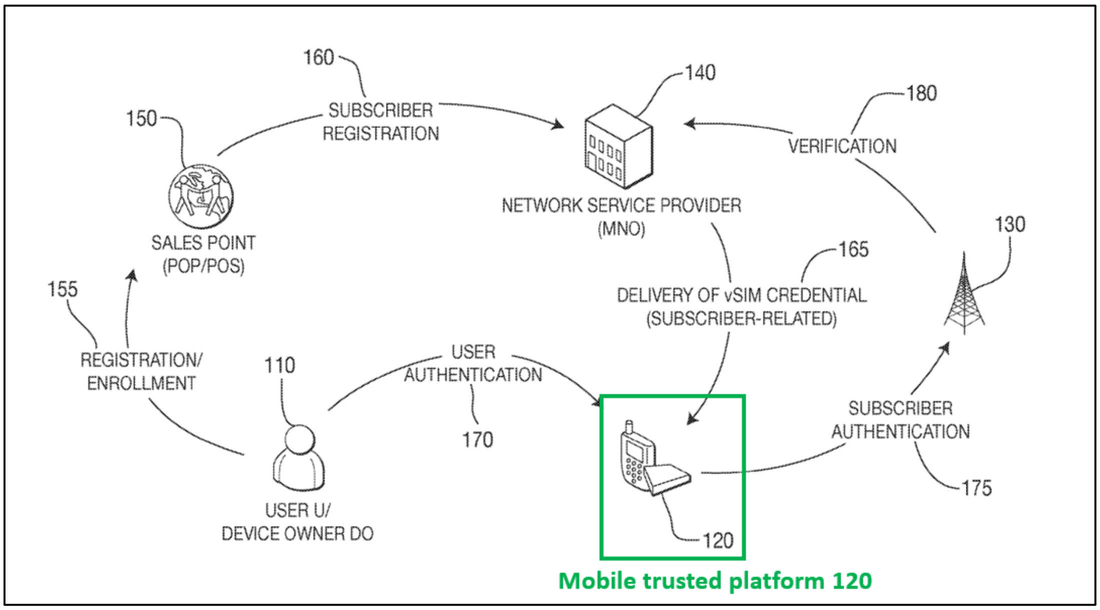
A. GROUND 1A – Schmidt-De Beer Renders Obvious Claims 1-3 and 8-12

1. Schmidt

Schmidt discloses a device architecture facilitating use of a "software-based access authorization credential," i.e., a virtual subscriber identity module (vSIM) credential, for wireless cellular network communications. SAMSUNG-1005, [0023]-[0024], [0026]-[0027].

Schmidt's system is implemented using a "'wireless transmit/receive unit

(WTRU)" that includes, e.g., "a user equipment (UE) ... a cellular telephone, ... or any other type of user device capable of operating in a wireless environment." SAMSUNG-1005, [0023]. FIG. 1 (below) shows a mobile device, which implements a mobile trusted platform (MTP) 120, included in a communication system architecture that uses "services and determine[s] subscriber identity" using a vSIM. SAMSUNG-1005, [0024]; SAMSUNG-1003, ¶¶82-84; SAMSUNG-1029, 1.



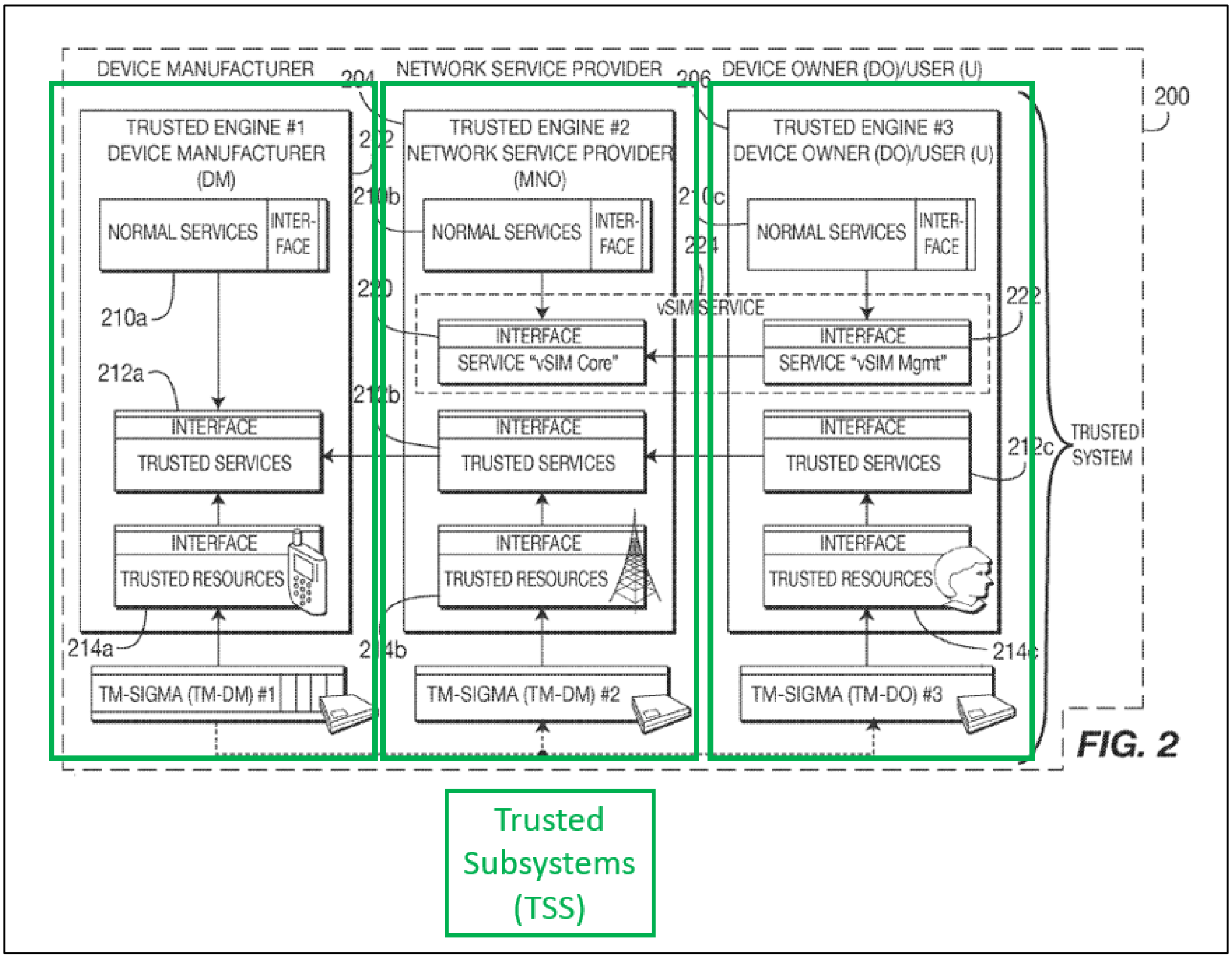
SAMSUNG-1005, FIG. 1 (annotated).

Schmidt's mobile trusted platform[2] (MTP) is configured to enable cellular network access and other vSIM services, including subscriber and network authentication, using a vSIM credential obtained from a Mobile Network Operator (MNO).

[2] Schmidt uses "mobile trusted platform" and "trusted mobile platform" interchangeably. *See, e.g.*, SAMSUNG-1005, [0024].

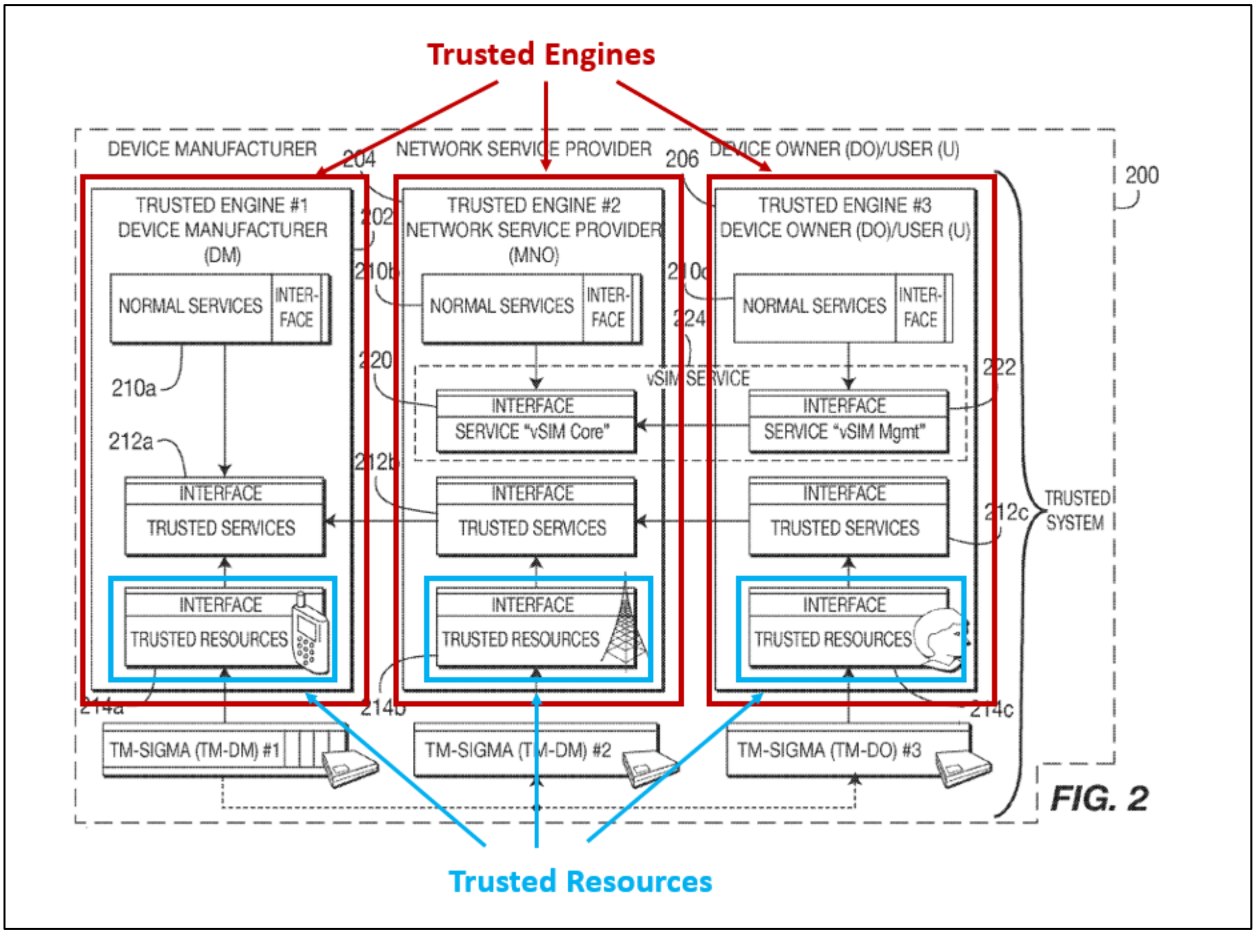
SAMSUNG-1005, Abstract, FIG. 1, [0024]-[0027], [0134]-[0142], FIG. 11.

Schmidt's vSIM architecture for an MTP (illustrated below) includes three trusted subsystems (TSSs) that operate on behalf of the device manufacturer (TSS-DM), the network service provider (TSS-MNO), and the device-owner/user (TSS-DO). SAMSUNG-1005, [0028].



SAMSUNG-1005, FIG. 2 (annotated); see also id., FIGS. 3-6 (similar environment).

Each trusted engine above includes trusted resources. SAMSUNG-1005, [0028], FIG. 2.



SAMSUNG-1005, FIG. 2 (annotated); see FIG. 3.

A POSITA would understand that trusted resources include, e.g., trusted or protected storage that is dedicated to the trusted engine/trusted subsystem. SAMSUNG-1005, [0040], [0099]; SAMSUNG-1003, ¶¶89-90; SAMSUNG-1030, FIG. 3, SAMSUNG-1032, [0003].

Each TSS has a particular role in device operation. TSS-DM provides "communications services" and "controls all internal and external communications and secures the communications channel." SAMSUNG-1005, [0032]. TSS-MNO manages "subscription-dependent and subscriber-related network provider services" e.g., GSM and data services. SAMSUNG-1005, [0026], [0033]; SAMSUNG-1003, ¶92. TSS-MNO is also "responsible for managing and protecting the subscriber-related portion of the vSIM credential," and performing network authentication of a subscriber. SAMSUNG-1005, [0033]. For this, TSS-MNO "provides the vSIM core service (vSIM-CORE)" that is "configured to substitute essential functions (subscriber authentication) for the conventional SIM" among "other authentication features." SAMSUNG-1005, [0033].

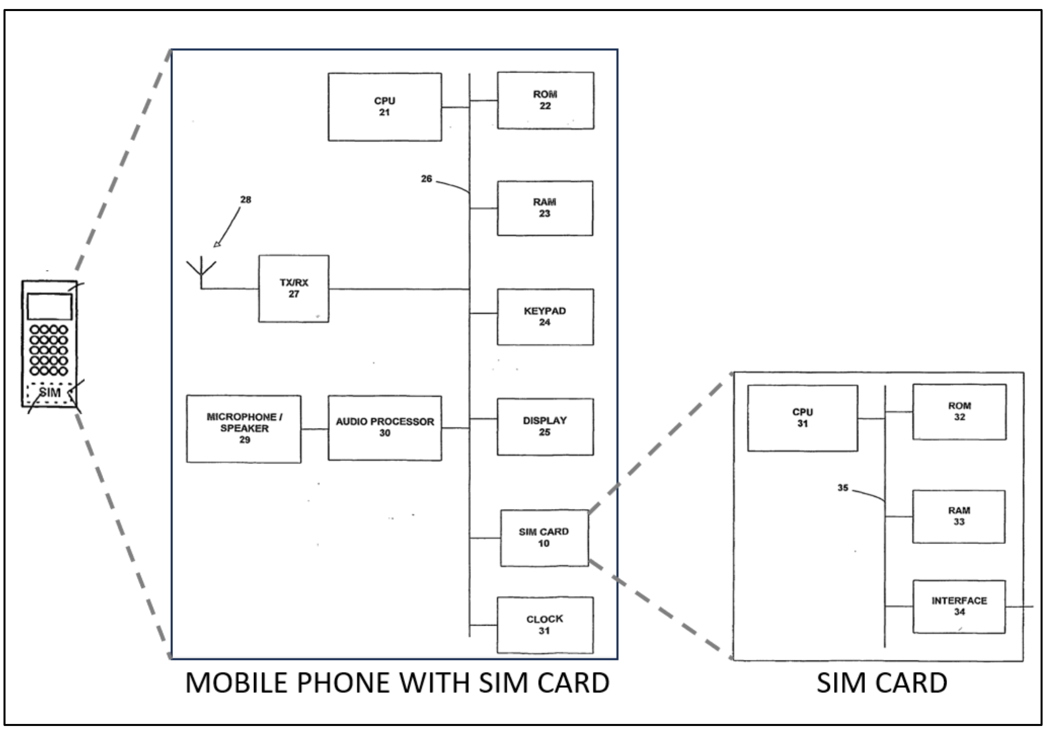
Each TSS includes a "trusted execution environment (TE-sigma)" and "security module (trusted module, TM) or the entity of the security module (TM-sigma) associated with the remote owner (RO) or stakeholder (sigma)." SAMSUNG-1005, [0031] ("Sigma" identifies DO/User, MNO or DM). Each TSS-sigma is "configured to sign and encrypt" data. SAMSUNG-1005, [0031].

After the vSIM is installed, the MTP uses the vSIM credential for subscriber authentication. SAMSUNG-1005, [0030], [0134]-[0142], FIG. 11. Once authenticated, the MNO provides services, e.g., GSM, data services, etc. SAMSUNG-1005, [0026].

2. De Beer (DB)

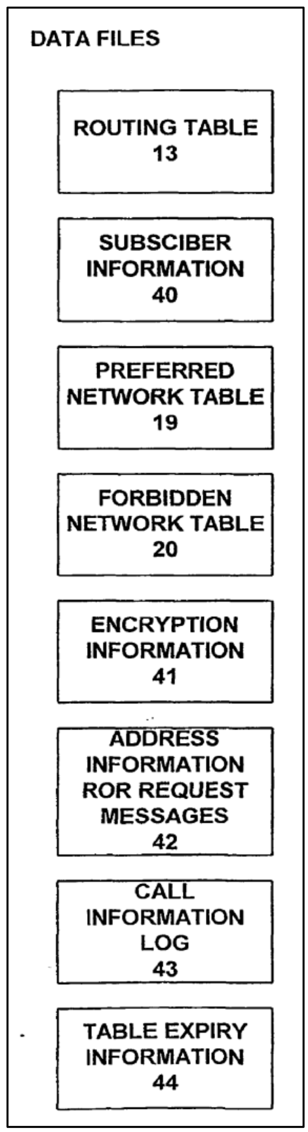
DB describes a mobile telephone that includes a SIM card to facilitate communications with "a cellular telecommunications system." SAMSUNG-1006, Abstract, [0043]. Using data stored in a SIM, DB's device "select[s] a network" for registration and "perform[s] optim[ized] call routing to a call destination." *Id.* Further, when data for a particular network is not present on the SIM, *e.g.*, when the device is roaming, the device retrieves the relevant data from a control centre. SAMSUNG-1006, Abstract, [0004].

DB's device (shown below) additionally includes a "transmitting and receiving circuit" that is "connected to an antenna" to facilitate network communications. SAMSUNG-1006, [0041]-[0044].



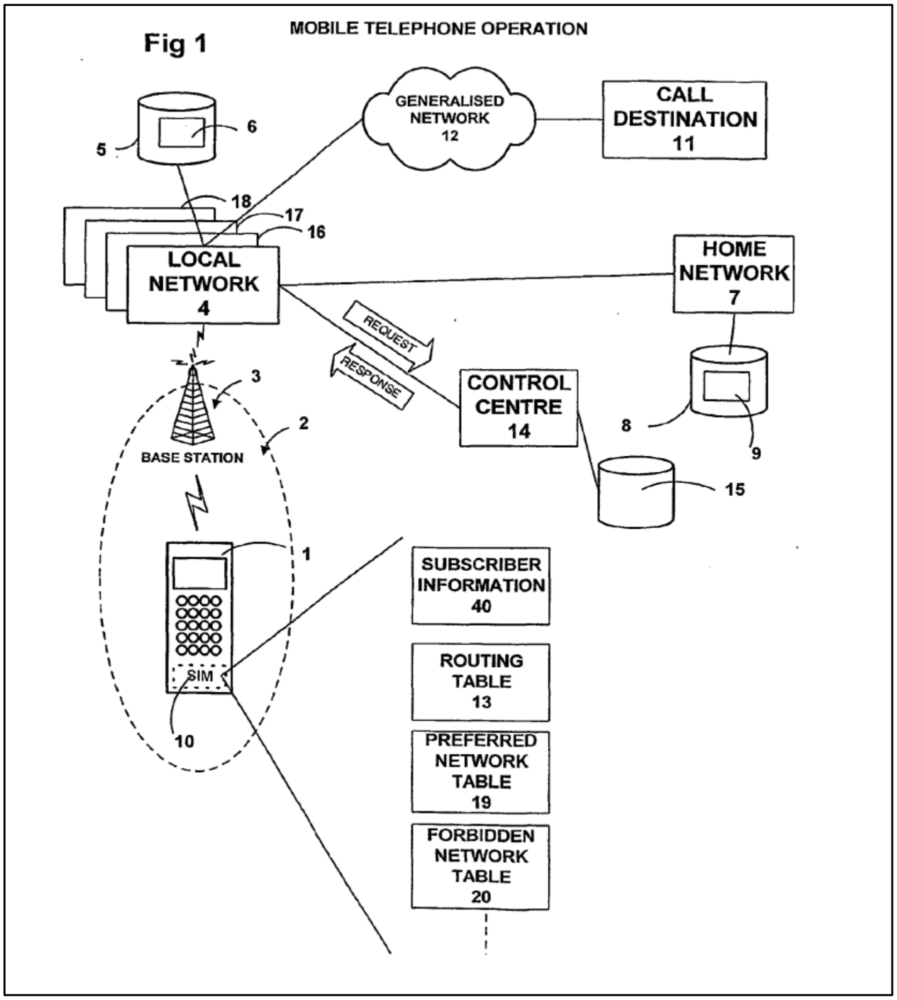
SAMSUNG-1006, FIGS. 1-3 (modified).

The SIM card stores—e.g., in its RAM memory—data files that guide device operation, including a routing table, subscriber information, preferred and forbidden network tables, call log, and table expiration information. SAMSUNG-1006, [0041], [0043], [0046]-[0051], FIG. 4; SAMSUNG-1003, ¶100.



SAMSUNG-1006, FIG. 4.

As illustrated in FIG. 1, when a device is outside its home network, it registers with a particular network (i.e., local network) selected from the available networks, "so that subsequent calls can be rapidly set up by the local network." SAMSUNG-1006, [0035].



SAMSUNG-1006, FIG. 1.

The mobile telephone selects a network from among available networks using data in lookup tables stored in the SIM's memory—namely, "a preferred network

table" listing "networks in order of preference" and "a forbidden network table" listing "networks for which the subscriber does not have authorisation from the home network" to use. SAMSUNG-1006, [0036], [0046].

Subsequently, "when a user enters a destination call number," an application on the phone "refer[s] to a lookup table" stored in the SIM's memory that "enables the mobile station to perform least cost routing" to the destination. SAMSUNG-1006, [0002]-[0003], Abstract, [0003], [0046]; SAMSUNG-1003, ¶104.

When the device roams from its home network, the "least cost routing" tables and the preferred and forbidden network tables, all stored on the SIM, may not include data for the currently available networks. SAMSUNG-1006, [0003]-[0004], [0039]. Additionally, the lookup tables include expiry information that "identif[ies] the maximum usable life of data such as the routing table," beyond which, the data are "expired and are no longer valid." SAMSUNG-1006, [0050], [0072]. When valid tables are unavailable, updated lookup tables are requested and obtained from a control centre, and these tables are used to connect to preferred networks and to facilitate least cost call routing. SAMSUNG-1006, [0005], [0051]-[0052], [0061], [0066]-[0069], [0033]-[0034], [0053].

To obtain the new tables from the control centre, the device generates a request message that is "transmitted as an SMS (Short Message Service) message via the local network" to the control centre. SAMSUNG-1006, [0067]. "The control

centre 14 responds by retrieving up-to-date tables" and transmitting "a response message" (SMS) sent "via the local network 4 to the mobile telephone." SAMSUNG-1006, [0067], [0072], [0108], [0110]. The device receives the response message and updates the tables on the SIM with the received data. *Id.*

DB's device additionally keeps a call log that stores "the duration and call destination of calls." SAMSUNG-1006, [0090]. The device periodically communicates the log data "to the control centre 14 by including call log information" in request messages. SAMSUNG-1006, [0090], [0101]. The control centre can use the log "to verify billing information generated by networks." SAMSUNG-1006, [0090].

3. Combination of Schmidt and De Beer

(a) <u>Overview</u>

Schmidt describes a mobile device implementing a vSIM service enabling access to and use of a wireless cellular network. §III.A.1; SAMSUNG-1003, ¶¶82-84, ¶111. The vSIM service "replaces conventional smart card-based SIM card and its function." SAMSUNG-1005, [0030]; §III.A.1; SAMSUNG-1003, ¶111. While Schmidt describes techniques for implementing the vSIM service that performs a traditional SIM card's functions of network use and access, it does not expressly describe how such conventional SIM-based function (e.g., making calls and connecting to cellular networks) is performed. SAMSUNG-1003, ¶112.

In the same field of cellular communications, DB describes implementation details regarding how these conventional SIM-based functions—including selecting a particular cellular network and routing calls efficiently—are performed using data stored in SIM memory. SAMSUNG-1006, Abstract; §III.A.2; SAMSUNG-1003, ¶113.

As explained below, given that Schmidt's vSIM service replaces a SIM card and its associated functions, a POSITA would find it obvious to combine Schmidt's and DB's teachings such that conventional SIM operations, e.g., network connection and call routing—per DB—would be performed using Schmidt's vSIM service and associated data. SAMSUNG-1003, ¶114.

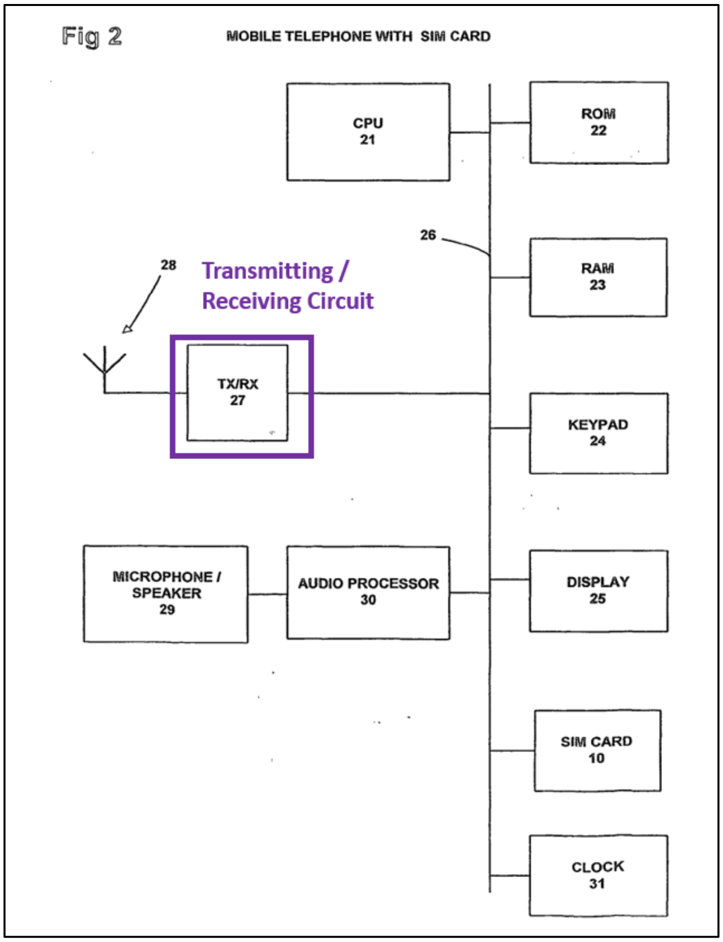
(b) <u>Facilitating wireless network communications using a wireless modem</u>

Both Schmidt and DB teach mobile devices that connect to and communicate with wireless cellular networks. §III.A.1-2. A POSITA would understand, or at least find obvious, that such mobile devices implement a modem to facilitate such wireless network communications. SAMSUNG-1003, ¶115.

Further, it was well-known for a mobile device to implement a modem to enable wireless cellular network communications. SAMSUNG-1003, ¶116. For example, Taylor describes a "***wireless radio modem***" and "***includes radio frequency***

modulation/demodulation circuitry." SAMSUNG-1026, Abstract.[3] Similarly, Schmidt and DB teach mobile devices with transmission and receiver circuitry to facilitate wireless network communications. §III.A.1-2; SAMSUNG-1003, ¶116. Schmidt describes a wireless transmit/receive unit (WTRU) that includes/implements a "radio frequency transceiver." SAMSUNG-1005, [0023], [0045]. DB similarly describes a mobile telephone with a "transmitting and receiving circuit," which is used when the processor "initiates a call setup procedure with the local network 4 by outputting signals via the transmitter." SAMSUNG-1006, [0041]-[0042], [0076]; SAMSUNG-1003, ¶116.

[3] Emphasis added throughout unless otherwise noted.



SAMSUNG-1006, FIG. 2 (annotated).

A POSITA would find it obvious for a computing device to use known networking components, such as a modem, to achieve the predictable result of facilitating network communications, as Schmidt and DB contemplate. SAMSUNG-1003, ¶117; *KSR v. Teleflex, 550 U.S. 398, 417 (2007)*. Using a modem to enable a user device to communicate over the wireless cellular networks would have been a conventional and obvious way to implement what each of Schmidt and DB describe, and is nothing more than utilizing familiar, known components (e.g., a modem with

the radio frequency transceiver of Schmidt, the TX/RX of DB) to achieve a predictable result of facilitating wireless cellular communications. SAMSUNG-1003, ¶117.

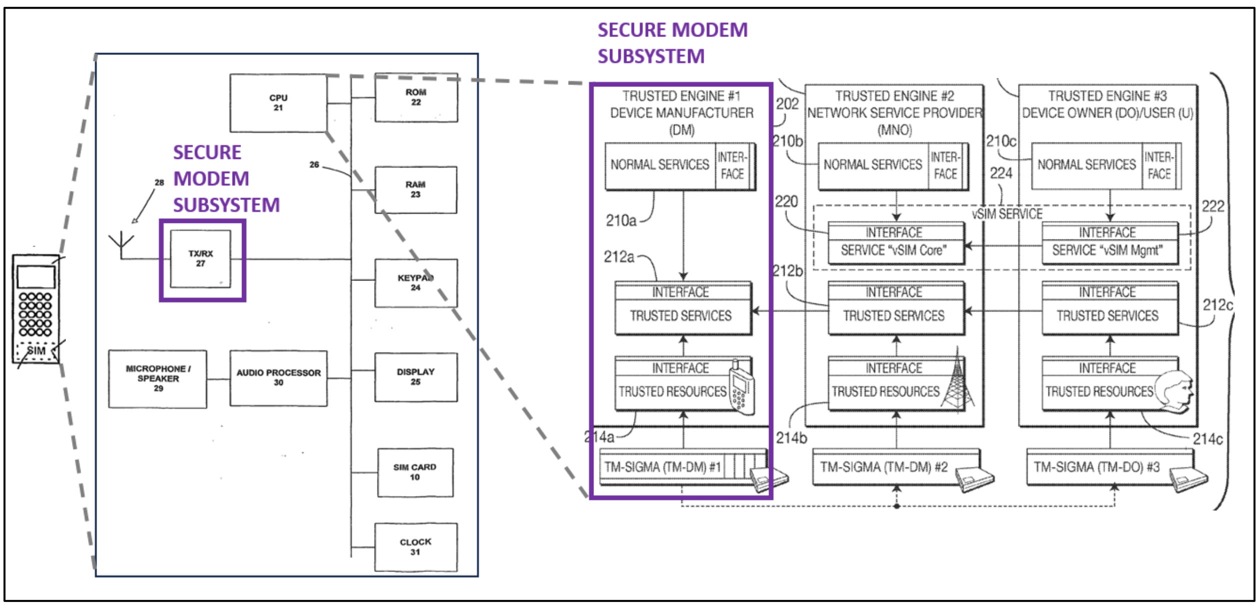
Thus, in view of Schmidt and DB's teachings and the knowledge of a POSITA (per Taylor's above-cited disclosures), a POSITA would understand or find obvious to implement a modem in Schmidt's mobile device to enable network communications. SAMSUNG-1003, ¶118. A POSITA would have reasonably expected success in implementing the mobile device with a modem (including the above-described TX/RX or transceiver components) because this was a well-known, conventional way of achieving the wireless cellular communications that Schmidt and DB describe. SAMSUNG-1003, ¶¶118-119; SAMSUNG-1034, [0028]-[0029], [0052]; SAMSUNG-1035, [0018].

(c) Securing transmissions from the modem

As explained in §III.A.3.b, the mobile device would implement a modem, including components such as a transceiver (e.g., TX/RX circuitry) that facilitate wireless cellular network communications. Because Schmidt teaches that TSS-DM—one of Schmidt's multiple separate, trusted execution environments—"controls all internal and external communications and secures the communications channel," a POSITA would understand or find obvious that the TSS-DM would control the communications transmitted/received via the above-described modem. SAMSUNG-

1005, [0025], [0031]-[0032]; SAMSUNG-1003, ¶121.

It was well-known for a device to include logic to control such wireless cellular communications via the modem (and its associated transceiver circuitry). *See* SAMSUNG-1003, ¶121; SAMSUNG-1034, [0027], [0052]. A POSITA would thus recognize that the TSS-DM (as executed by a processor, e.g., device's CPU (per DB)) and the above-described wireless modem together make up a modem subsystem, as illustrated below. SAMSUNG-1003, ¶122.



SAMSUNG-1005, FIG. 2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified), SAMSUNG-1003, ¶122.

Additionally, because TSS-DM controls the communications and "secures" the channels used for such communication, a POSITA would recognize that the TSS-

DM together with the modem's transceiver circuitry, make up the combination device's secure modem subsystem. SAMSUNG-1003, ¶123. Indeed, further illustrating the secure aspects of the TSS-DM, Schmidt explains that an MTP "support[s] ***multiple protected, separate execution environments***"—one of which is the TSS-DM—where "[e]ach environment represents an area associated with a stakeholder." SAMSUNG-1005, [0030]. A POSITA would recognize that using multiple TSSs, one for each stakeholder, isolates and protects data associated with the different stakeholders. SAMSUNG-1003, ¶¶123-124.

Implementing the combination's secure modem subsystem would thus have been a conventional and obvious way to implement secure communications using a wireless modem and is nothing more than utilizing familiar, known components (e.g., a modem including RF circuitry of Schmidt and DB, together with TSS-DM of Schmidt) to achieve a predictable result of facilitating secure wireless cellular communications from the device. SAMSUNG-1003, ¶125.

A POSITA would have reasonably expected success in implementing such a secure modem subsystem given (1) Schmidt and DB's teachings of circuitry making up a modem enabling cellular network communications, (2) the common use of logic executed by a device to control communications using these hardware components, and (3) Schmidt's additional teachings of TSS-DM—i.e., a software-based TSS ex-

ecuted by a device processor—that provides one example of such conventional processing logic that controls network communications and additionally secures such communications. SAMSUNG-1003, ¶126.

(d) Providing a secure partition in device memory that stores data conventionally stored in a physical SIM's memory

As explained in §III.A.1 *supra*, Schmidt's system would include a mobile device (e.g., cellular telephone) that implements an MTP and which includes a storage medium in the form of different types of memory. *See* SAMSUNG-1005, [0023], [0143]-[0145]; SAMSUNG-1003, ¶127; SAMSUNG-1029, 1; SAMSUNG-1032, [0003].

As explained in §III.A.1, the MTP includes multiple TSSs each configured to "store" information related to that subsystem. SAMSUNG-1005, [0005]. For example, the TSS-MNO "includes a vSIM core services unit, configured to ***store***, provide and process credential information relating to the MNO," and the "TSS-DO/TSS-U includes a vSIM management unit, configured to ***store***, provide and process credential information relating to the user of the MTP." *Id.*

Schmidt teaches that the architecture provides a "***protected storage***." SAMSUNG-1005, [0040], [0099]. Indeed, the "vSIM core service"—which is part of the TSS-MNO—is responsible for "the ***secure storage*** and use of subscribed data as well as subscriber authentication with the MNO." SAMSUNG-1005, [0033].

A POSITA would recognize that providing a "protected storage" in a vSIM

environment—as disclosed in Schmidt—offers some of the same security characteristics offered by a conventional SIM card. SAMSUNG-1003, ¶129; SAMSUNG-1029, 6; SAMSUNG-1066, [0028], [0035], [0046], FIG. 3.

For these and the below reasons, a POSITA would find obvious to implement Schmidt's "protected storage" as one or more secure memory partitions within on-device memory.[4] SAMSUNG-1003, ¶130.

First, as explained above, secure memory has significant security benefits that include, e.g., preventing circumvention of network access control mechanisms, preventing leakage of sensitive information, and ensuring proper operation of network services. SAMSUNG-1003, ¶131; SAMSUNG-1029, 6. Indeed, to provide the vSIM service that includes the same security benefits of a physical SIM, Schmidt's device is configured to provide "protected" or "secure" storage for storing SIM-related information (as explained above). SAMSUNG-1005, [0040], [0099]; SAMSUNG-1003, ¶131. Therefore, a POSITA would understand that the combination's device includes secure memory. SAMSUNG-1003, ¶131.

Second, and relatedly, it was well-known for device memory to include a secure memory partition to achieve such secure memory or protected storage within

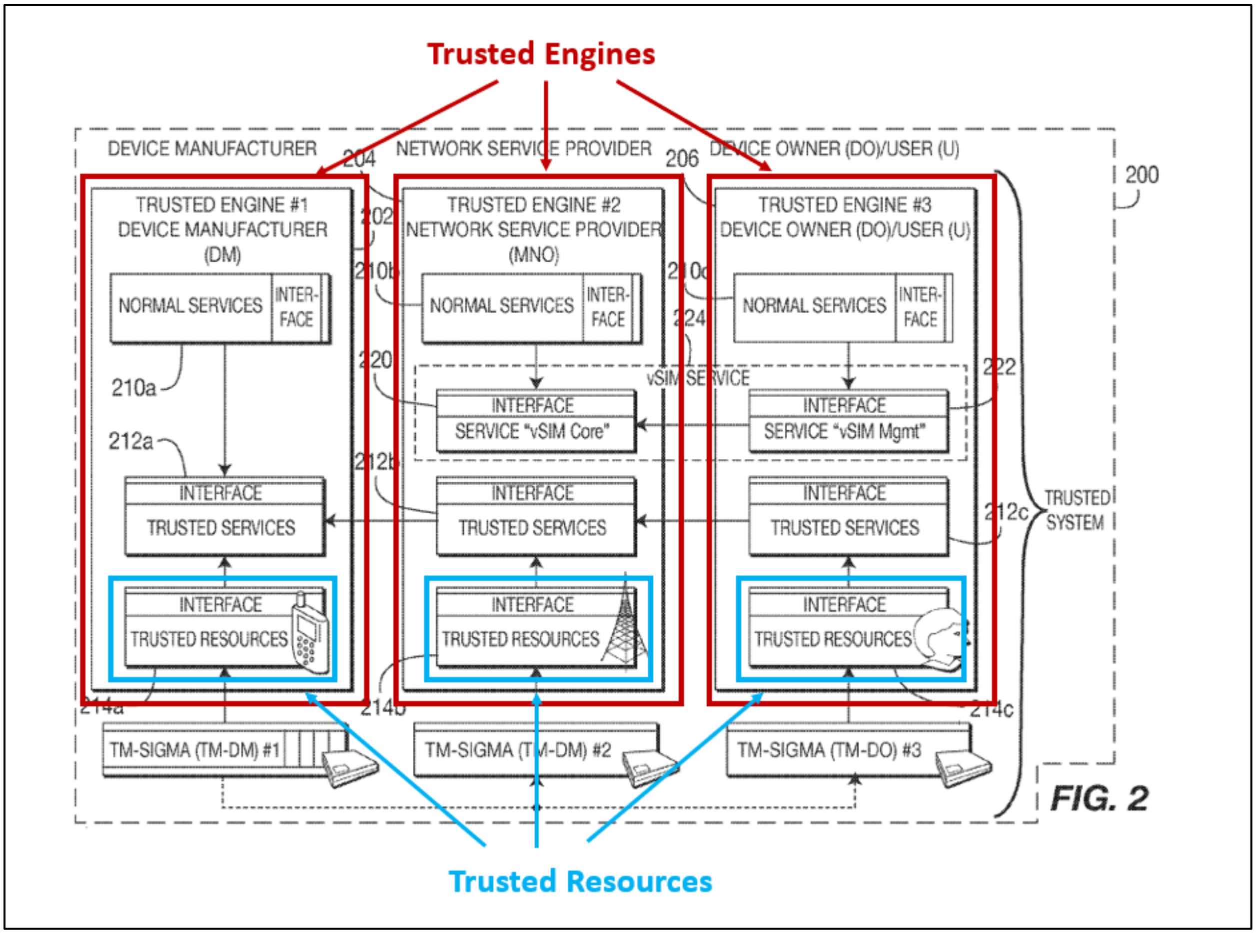
---

[4] In mobile devices, secure memory (e.g., flash memory) is secure storage. SAMSUNG-1003, ¶131.

on-device memory. SAMSUNG-1003, ¶132; SAMSUNG-1028, [0019]-[0020], FIG. 2.

Third, it was well-known for access to a secure memory partition to be limited to a secure execution environment (SEE) and doing so, offered security benefits, including preventing unauthorized access to secure data, e.g., by misusing direct memory access and/or processor capabilities. SAMSUNG-1003, ¶133; SAMSUNG-1028, [0004].

Fourth, Schmidt illustrates that each trusted engine (which are components of the trusted subsystems, TSS-DM, TSS-MNO, TSS-DO/U) has access, via a dedicated interface, to a set of dedicated trusted resources. SAMSUNG-1005, [0037], FIG. 2; SAMSUNG-1003, ¶134.



SAMSUNG-1005, FIG. 2 (annotated)

It was well-known for access to trusted resources to be limited to a particular secure execution engine and to include secure storage. SAMSUNG-1003, ¶¶135-136; SAMSUNG-1030, FIG. 3.

Since Schmidt illustrates that the trusted resources (including protected/secure storage) in a trusted engine are accessed only by trusted services in that engine, a POSITA would have recognized or found obvious that access to a protected storage/secure memory partition would be limited to the corresponding trusted engine. SAMSUNG-1003, ¶137; SAMSUNG-1030, 28, FIG. 3; SAMSUNG-1005, FIGS. 2.

Thus, to achieve Schmidt's goal of providing "a more dynamic and ***concurrently secure*** software based solution to the SIM function," a POSITA would have been motivated to provide a secure partition in on-device memory to facilitate such protected and dedicated storage of subscriber and other similar SIM-related data, as Schmidt contemplates. SAMSUNG-1005, [0004]; SAMSUNG-1003, ¶¶138-140.

Implementing such a secure memory partition as part of Schmidt's on-device memory would have been nothing more than implementing known methods/techniques (providing a secure memory partition for on-device memory) to known systems/devices (Schmidt's MTP/device that already contemplates a protected storage accessible by its TSSs) to achieve predictable results (a device with multiple TSSs and a memory with dedicated secure memory partitions, one which stores the SIM and subscriber related information). SAMSUNG-1003, ¶140.

A POSITA would have had a reasonable expectation of success in so implementing one or more secure memory partitions within memory of Schmidt's device because (1) Schmidt's MTP includes a "protected storage" function and on-device memory, (2) TSS-MNO, via its vSIM core service, is responsible for "secure storage and use of subscriber data as well as subscriber authentication with the MNO," and (2) it was well-known and conventional to use secure memory partitions to facilitate such secure storage within on-device memory (e.g., that is accessible by a respective TSS). SAMSUNG-1003, ¶141. Such a combination would have been well within a

POSITA's capability to implement and would have involved a known and conventional implementation that achieves the MTP's disclosed secure data storage and access functions. SAMSUNG-1003, ¶141.

Moreover, a POSITA would have had multiple reasons to store data—conventionally stored in a physical SIM card–in one or more of the above-described secure memory partitions that would have been implemented in Schmidt's on-device memory. SAMSUNG-1003, ¶142.

In Schmidt, TSS-MNO's "vSIM core service is responsible for the ***secure storage*** and use of ***subscriber data as well as subscriber authentication*** with the MNO." SAMSUNG-1005, [0033]. A POSITA would understand or find obvious that such "subscriber data" and "subscriber authentication" related information are used together with a network operator (MNO) and would include data conventionally stored in a physical SIM's memory and used to access/use wireless services provided by a network operator. SAMSUNG-1003, ¶143. Further, as described above, storing subscriber data in secure memory prevents circumvention of network access control mechanisms and prevents leakage of sensitive information. SAMSUNG-1003, ¶143, SAMSUNG-1029, 6. Therefore, a POSITA would understand/find obvious that vSIM subscriber data is stored in the secure memory partition. SAMSUNG-1003, ¶143.

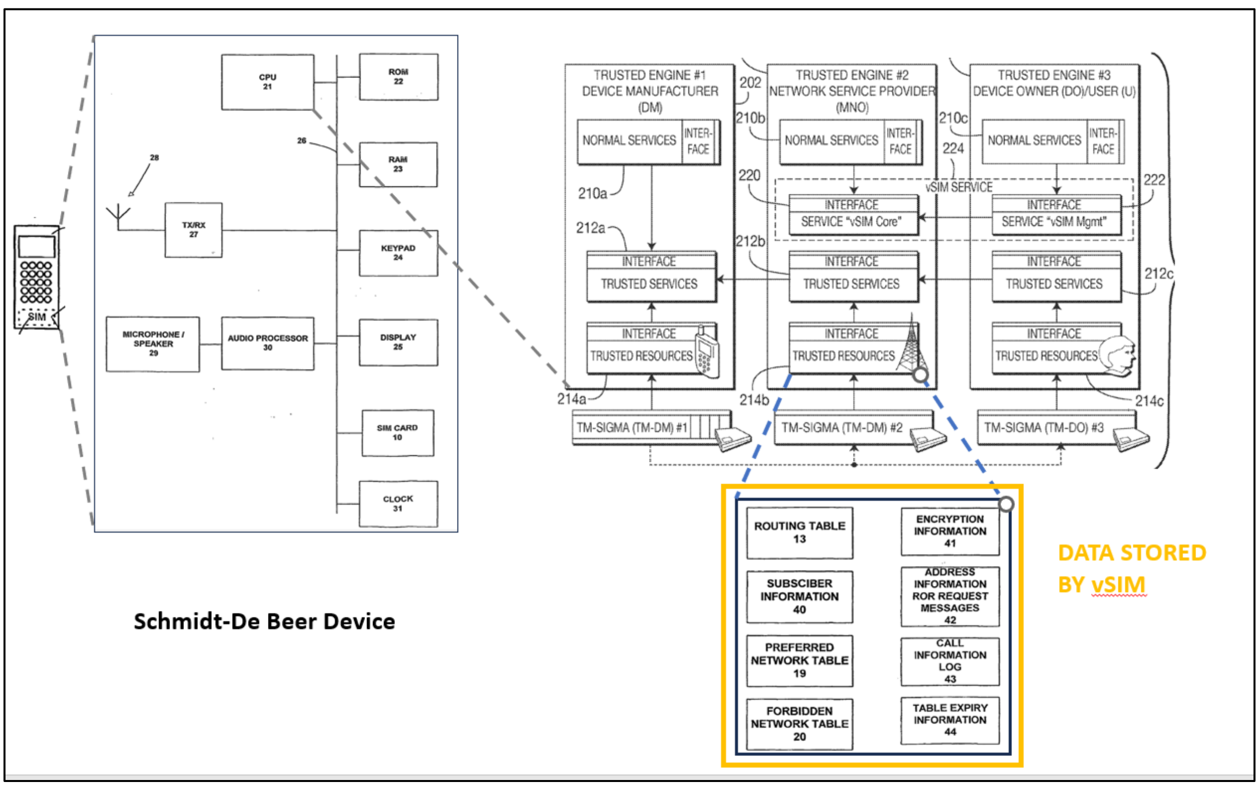
Further, DB disclosed a SIM's memory storing data (e.g., a routing table, preferred and forbidden network tables, etc.) used to connect to a cellular network that provides voice service (e.g., calling using the connected-to network). *See* SAMSUNG-1006, [0005], [0034], [0038], [0046], [0050]-[0051], FIG. 4; SAMSUNG-1003, ¶144; SAMSUNG-1025, 15-16, 19-22, 24-27, 32, 34-35, 39.

A POSITA would have had multiple reasons for the one or more above-described secure memory partition(s) to store SIM data such as DB's lookup tables, given Schmidt's disclosure of secure storage of similar information and DB's disclosure of storing such information in the SIM's dedicated memory. SAMSUNG-1003, ¶145. Indeed, providing secure storage of such information would further Schmidt's security goal of "prevent[ing] loss and escape of security-sensitive data, and ensur[ing] that all necessary services"—such as wireless network access and use of voice services—"are available and functional." SAMSUNG-1005, [0040].

Additionally, Schmidt teaches that its vSIM service "replaces the conventional smart card-based SIM card and its function." SAMSUNG-1005, [0030]. Therefore, to enable Schmidt's vSIM service to replace conventional SIM card function, it would have been obvious for this service to store data conventionally stored in a physical SIM's memory, such as the above-described tables in DB (as illustrated below). SAMSUNG-1003, ¶146.

This combination would have thus amounted to implementing known methods/techniques (storing SIM data in a secure on-device memory partition) to known systems/devices (Schmidt's vSIM-based MTP) to achieve predictable results (usage of vSIM services that are the same as those offered by a physical SIM). SAMSUNG-1003, ¶147.

A POSITA would have further expected reasonable success in such a combination given Schmidt's teaching of secure storage of data used to communicate with a network operator, and DB's express recognition of such data including the above-described lookup tables. SAMSUNG-1003, ¶148.



SAMSUNG-1005, FIG. 2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified), SAMSUNG-1003, ¶¶138-148.

(e) Implementing roaming capability in Schmidt's vSIM-based environment

Schmidt's MTP uses the vSIM service to access wireless cellular network services—similar to how a physical SIM facilitates connection and access to network services. SAMSUNG-1005, [0093]-[0109], FIG. 8; SAMSUNG-1003, ¶149. Additionally, as explained in §III.A.3.d, a POSITA would find it obvious to store data conventionally stored in SIM memory, within a secure memory partition on the combination's device. SAMSUNG-1003, ¶149.

Although Schmidt does not expressly describe how cellular services are used when the device is roaming, a POSITA would have had multiple reasons to implement the device to facilitate use of network services while roaming and would have leveraged DB's teachings in this regard. SAMSUNG-1003, ¶150.

First, it was well-known for devices communicating over wireless cellular network communications to support cellular network access and services while the device is roaming. SAMSUNG-1003, ¶151, SAMSUNG-1027, Abstract, 2:10-16.

A POSITA would have been motivated to implement such conventional roaming functionality within a mobile device to, e.g., enable device mobility away from a home network without interrupting access to wireless network services (e.g., calling over a cellular network when roaming). SAMSUNG-1003, ¶152.

Second, per DB, a device has insufficient memory to store, for all regions, the

relevant routing information, preferred and forbidden network tables. SAMSUNG-1006, [0003]-[0005], [0046]-[0051], [0066]-[0074]; SAMSUNG-1003, ¶153. Therefore, in DB, the device determines whether new tables are required, and if so, uses the local network to retrieve up-to-date tables from a control centre and stores the updates in the SIM's memory. SAMSUNG-1006, [0061], [0066]-[0074]. Then, using the data in the updated lookup tables, DB's system accesses a preferred wireless network and performs least cost routing for calls. SAMSUNG-1006, [0068]-[0069], [0033]-[0034], [0053]; SAMSUNG-1003, ¶154.

A POSITA would have thus been motivated to leverage DB's above-described teachings to overcome the issues with outdated SIM data, by obtaining and updating the lookup tables stored in secure memory and using that data to enable access to preferred wireless networks and to perform least cost routing of a call to its destination, including while the device is roaming. SAMSUNG-1003, ¶155; SAMSUNG-1006, [0036], [0038], [0046], [0057], [0075], [0084], [0087], [0097], [0099]-[0100], [0112].

Third, implementing DB's teachings in combination with Schmidt would have amounted to nothing more than the use of a known technique (enabling conventional roaming functionality via DB's described teachings of updating lookup tables stored in the SIM and leveraging that data to facilitate network access and use while roaming) to improve similar devices (Schmidt's MTP) in a similar way and

combining prior art elements according to known methods to yield predictable results (as described above, e.g., network connectivity and least cost routing when roaming). SAMSUNG-1003, ¶156.

A POSITA would have expected success in implementing DB's teachings related to roaming into Schmidt's device. SAMSUNG-1003, ¶157. The elements of the resulting combination device would each perform functions they had been known to perform prior to combination—the Schmidt-DB device providing for secure storage of lookup tables in a secure memory partition and DB's teachings of updating the data and using that data for network connectivity and call routing while the device is roaming. SAMSUNG-1003, ¶157. Moreover, combining these teachings would have required only routine programming knowledge well within a POSITA's skill. SAMSUNG-1003, ¶157. Schmidt already teaches that its TSS-MNO securely accesses stored data to interact with a network operator, and thus, it would be straightforward to configure the TSS-MNO to interact with a network operator (e.g., control centre), to obtain updated data and implement the additional functionality that uses this data to perform the above-described services (per DB). SAMSUNG-1003, ¶157.

(f) Schmidt-DB Combination

Schmidt-DB Device (SDD) refers to the above-described system that a

POSITA would have been led to form based on Schmidt's and DB's teachings. SAMSUNG-1003, ¶158.

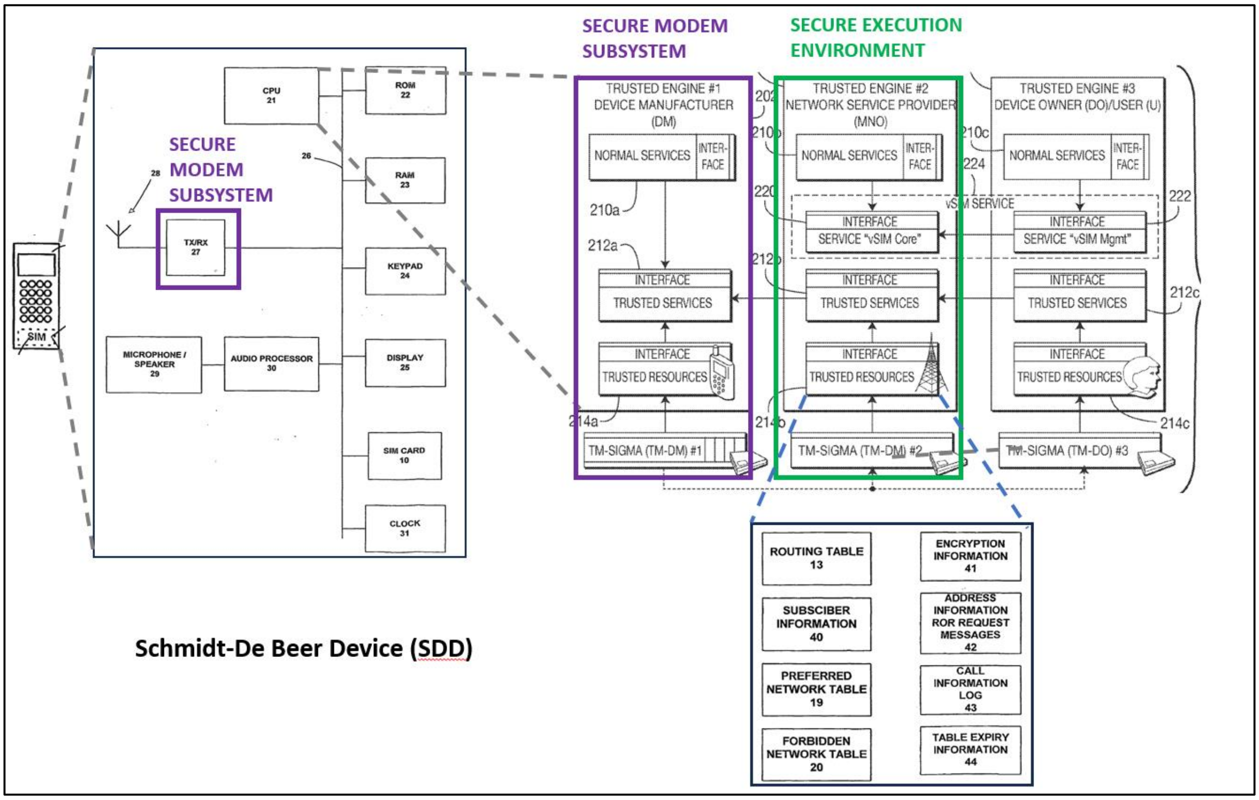
SDD implements a mobile device that, per Schmidt, includes an MTP with multiple trusted subsystems (TSS-DM, TSS-MNO, TSS-DO) and stores a vSIM credential. SAMSUNG-1005, [0002], [0023]-[0024], [0029]-[0035], Abstract; SAMSUNG-1003, ¶159; *see* §III.A.1.

SDD's mobile device further includes a wireless modem, including transceiver components, such as TX/RX, per DB and Schmidt. SAMSUNG-1006, [0042], FIG. 2; SAMSUNG-1003, ¶160.

The wireless modem is secured by TSS-DM, which, per Schmidt, "***controls*** all internal and external communications and ***secures the communications channel***." SAMSUNG-1005, [0032]; SAMSUNG-1003, ¶161. SDD's wireless modem (including the transceiver components) and TSS-DM together serve as a secure modem subsystem that facilitates the device's network communications. SAMSUNG-1003, ¶161.

SDD includes one or more secure memory partitions in on-device memory, and stores therein the vSIM credential (per Schmidt), as well as additional information conventionally stored on a physical SIM—which, per DB—include a routing table, preferred network table, forbidden network table, etc. SAMSUNG-1006, [0046]-[0051], FIG. 4; SAMSUNG-1003, ¶162.

An example architecture of SDD, which leverages Schmidt and DB's teachings, is illustrated below:



SAMSUNG-1005, FIG. 2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified), SAMSUNG-1003, ¶163.

Additionally, as described above, SDD leverages DB's teachings related to roaming. SAMSUNG-1003, ¶164. For example, when away from its home network and after connecting with a local network, SDD determines whether new tables are required, and if so, uses the local network to retrieve up-to-date tables from a control centre and stores them in secure memory (per DB). SAMSUNG-1006, [0061], [0066], [0067]; SAMSUNG-1003, ¶164. Additionally, per DB, SDD is configured

to update this data (stored in a secure memory partition in SDD) and use this data for network functions, such as connecting to a preferred network and performing least cost routing to a call destination. SAMSUNG-1006, [0052]-[0053], [0056]-[0059], [0068]; SAMSUNG-1003, ¶¶164-165.

4. Analysis

[1.1]

SDD renders obvious a method of operating a wireless end-user device. SAMSUNG-1003, ¶¶194-197.

SDD is a wireless end-user device. SAMSUNG-1003, ¶195. Per Schmidt, SDD is a "wireless transmit/receive unit (WTRU)" that includes "a cellular telephone" and "any other" "user device capable of operating in a wireless environment." SAMSUNG-1005, [0023]. Similarly, DB teaches that a mobile telephone "in a cellular telecommunications system uses" data stored in lookup tables to select a network "for registration and to perform optimize[d] call routing." SAMSUNG-1006, Abstract.

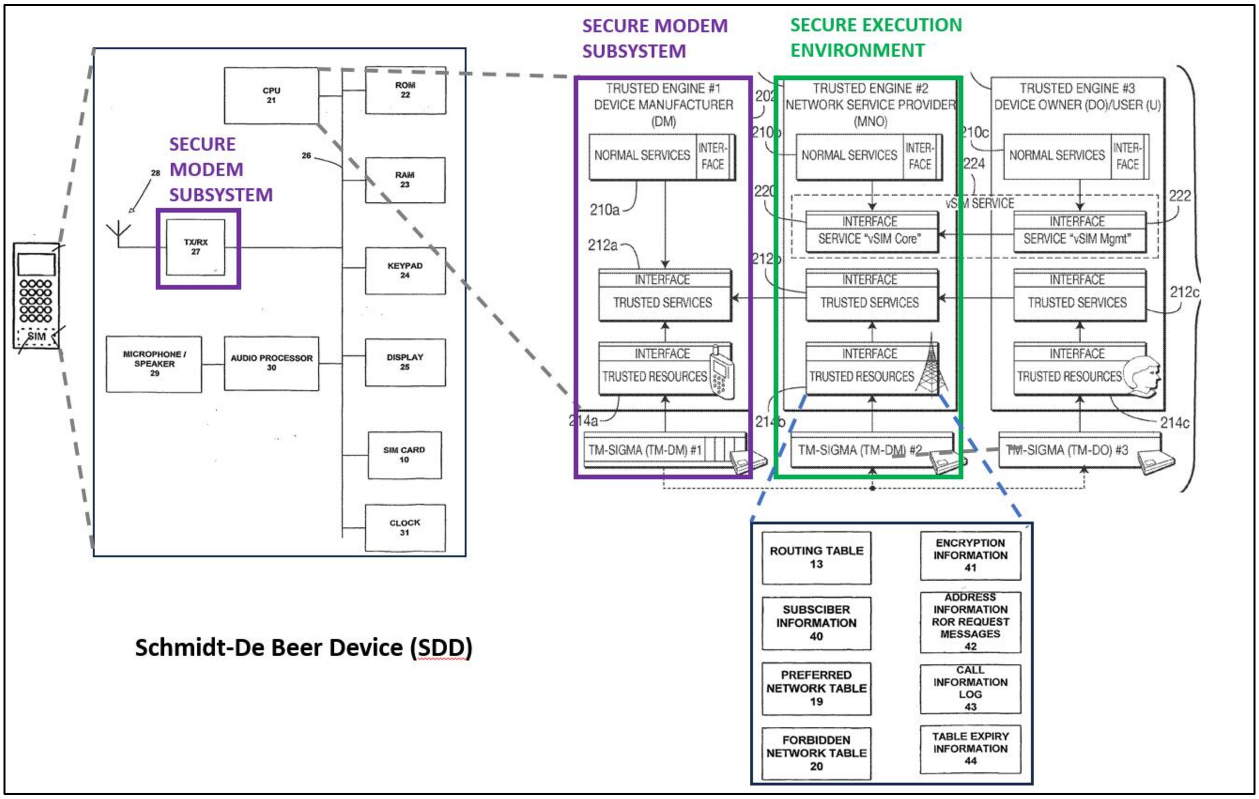
As explained in §§III.A.3.d-e, the methods of operating SDD include (1) storing and updating the routing, preferred network and forbidden network tables in the device's secure memory partition, and (2) using these tables to connect to appropriate networks and using services (e.g., making calls over these networks, using least cost routing as determined using the lookup tables (per DB), etc.). SAMSUNG-

1005, [0030]; SAMSUNG-1006, [0038], [0066]-[0077], FIG. 4; SAMSUNG-1003, ¶197. Additional details regarding the above-described methods for operating SDD are described with reference to [1.2]-[1.7] (incorporated here).

[1.2]

SDD's operation renders obvious connecting from a secure modem subsystem (e.g., SDD's secure modem subsystem including transceiver circuitry and TSS-DM) to a wireless cellular network (e.g., local network). SAMSUNG-1003, ¶¶198-204.

As explained in §§III.A.3.b-c, SDD includes a secure modem subsystem, which includes TSS-DM and transceiver circuitry (e.g., TX-RX circuitry). SAMSUNG-1003, ¶199. Also, as explained in §III.A.3.c, TSS-DM together with the transceiver circuitry is a secure modem subsystem because TSS-DM secures the communication channels used for external communications from the device. SAMSUNG-1005, [0032]; SAMSUNG-1003, ¶199.



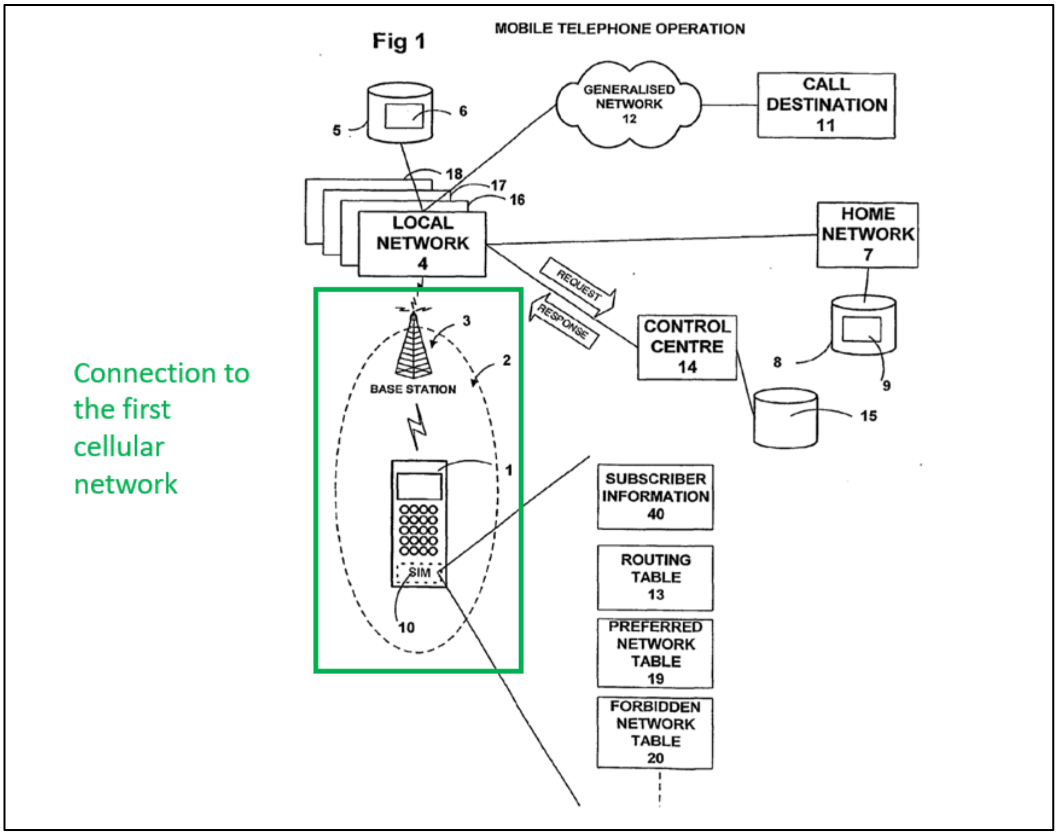
SAMSUNG-1005, FIG. 2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified), SAMSUNG-1003, ¶¶198-199.

SDD connects to the wireless cellular network from the secure modem subsystem. *See* §III.A.3; SAMSUNG-1003, ¶200. Per Schmidt (further described in [1.1]), SDD is a mobile device (e.g., a cellular telephone, PDA) which implements a "procedure for allowing access of a communication subscriber 802 to a ***cell based communication network***" (i.e., wireless cellular network) "using the software based authorization credentials of the trusted mobile platform." SAMSUNG-1005, [0093], [0023]-[0024]; SAMSUNG-1003, ¶200; *see* §III.A.3. Additionally, per Schmidt, TSS-DM "generally controls all internal and external communications," and "all

protocol messages of a TSS-sigma are transmitted by" its communications services. SAMSUNG-1005, [0032].

Because TSS-DM controls ***all*** external communications of SDD, it would control communications to a wireless cellular network (as further explained below). SAMSUNG-1005, [0032]; SAMSUNG-1003, ¶201. Further, because TSS-DM is part of SDD's secure modem subsystem, a POSITA would understand that connections to the wireless cellular network are from SDD's secure modem subsystem. *See* §III.A.3.c; SAMSUNG-1003, ¶201. Additionally, the wireless cellular network communications controlled by TSS-DM would be transmitted/received by SDD's transceiver circuitry. SAMSUNG-1003, ¶201.

Further, per Schmidt and DB, SDD connects from a secure modem subsystem to a wireless cellular network. SAMSUNG-1005, [0102]; SAMSUNG-1006, [0027], [0061]; SAMSUNG-1003, ¶202. This is illustrated below:



SAMSUNG-1006, FIG. 1 (annotated).

As DB explains, "the mobile telephone 1 is currently located within a cell 2 served by a base station 3 of a local network 4" that is "***accessible via cellular broadcast***." SAMSUNG-1006, [0027]. "When the mobile telephone 1 is turned on, it… register[s] with the local network." SAMSUNG-1006, [0035]. A POSITA would understand that registering with the local network (which is a wireless cellular network) is connecting to that network. SAMSUNG-1003, ¶203.

Thus, SDD leverages DB's and Schmidt's above-referenced teachings, such that during operation, SDD connects to a wireless cellular network (e.g., the local

network that is accessible via cellular broadcast) from SDD's secure modem subsystem. SAMSUNG-1003, ¶204.

[1.3]

As explained below, SDD renders obvious connecting a first secure control channel (e.g., a channel over which an encrypted message is sent via SMS) from the secure modem subsystem (e.g., TSS-DM operating in conjunction with the TX/RX) through the wireless cellular network (e.g., local network) to a network service controller (e.g., control centre). SAMSUNG-1003, ¶¶205-214.

The '429 Patent does not define the terms "control channel" or "channel." *See* SAMSUNG-1001. A POSITA would recognize that a "channel" includes "a stream of information transmitted as part of a distinct communication, or conversation, or for a particular purpose or end use" and "[o]ne channel may be distinguished from other channels by the time of occurrence of the transmission," among other factors. SAMSUNG-1022, 3; SAMSUNG-1003, ¶206. A POSITA would further understand that a control channel includes a channel over which control information is transmitted. SAMSUNG-1003, ¶206, §VII.C.

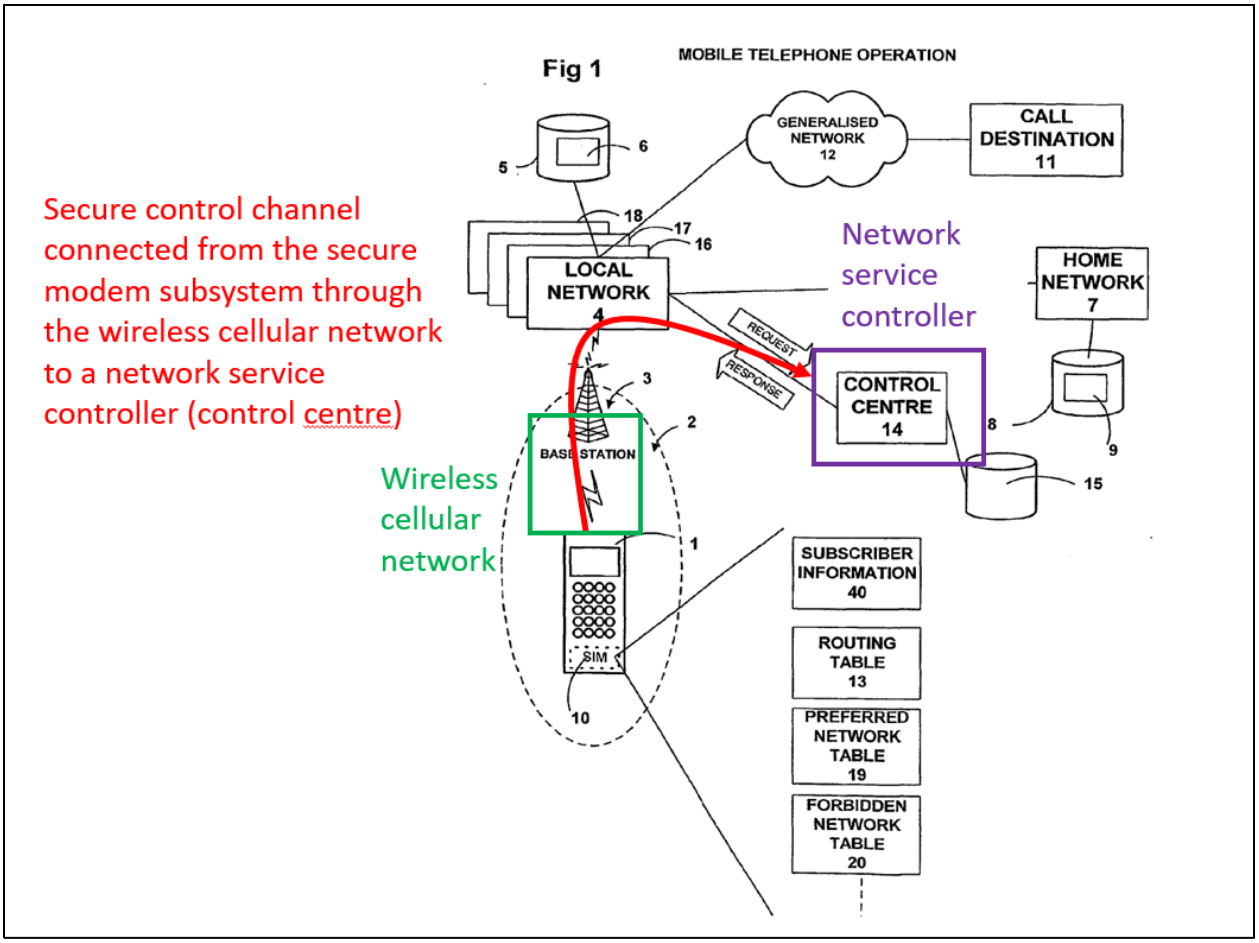
Consistent with this understanding, SDD renders obvious connecting a secure control channel through the wireless cellular network to a network service controller. SAMSUNG-1006, [0067]; SAMSUNG-1003, ¶207.

As explained in §III.A.3.e, SDD leverages DB's teachings of obtaining updated lookup tables including data regarding preferred and forbidden networks, and routing information—e.g., by requesting and receiving such information via an SMS message sent over a control channel. SAMSUNG-1003, ¶208. Per DB, after registering with the local network, SDD determines whether "the subscriber has moved to a location in a new country." SAMSUNG-1006, [0066]. If so, a request message is generated to obtain "new versions of the routing table 13, preferred network table 19 and the forbidden network table 20," and this message is "***transmitted as an SMS (Short Message Service) message via the local network***" (i.e., wireless cellular network) "***to the control centre*** 14." SAMSUNG-1006, [0067]; SAMSUNG-1003, ¶208.

The '429 patent explains that "service control policies, for example, can be set by the service controller." SAMSUNG-1001, 14:56-58. Since that function is performed by SDD's control centre, a POSITA would understand that the control centre is a network service controller. SAMSUNG-1003, ¶209. Additionally/alternatively, DB's control centre is also a network service controller because it controls network services (e.g., by providing routing tables that are used to access a network and its services). SAMSUNG-1003, ¶209; SAMSUNG-1033, 1:23-30.

The SMS messages to the control centre include control information and are distinct from data messages that are sent via SMS and displayed to the user. SAMSUNG-1003, ¶210. Per DB, such "SMS messages" sent/received by the device "[are] transparent to the [mobile telephone's] user" and constitute "a special type of SMS message" that is not "displayed in the [mobile phone's] display." SAMSUNG-1006, [0080]. These messages include requests for information or the actual information (e.g., routing table, preferred network table and forbidden network table), which control how the device accesses a network and therefore constitute control information. SAMSUNG-1003, ¶210. Thus, these special SMS messages include control information that are used to control the device, and the channel over which they are sent is therefore a control channel. SAMSUNG-1003, ¶210.

Additionally, a POSITA understands or finds obvious that the above-described special SMS message would be transmitted over a control channel. SAMSUNG-1003, ¶211. It was well-known for such SMS messages to be sent over control channels. SAMSUNG-1003, ¶211. For example, Minborg explains that "[i]n the GSM standard, ***SMS messages can be transmitted over a Stand-alone Dedicated <u>Control Channel</u>*** (SDCCH)." SAMSUNG-1020, [0005]; *see* SAMSUNG-1021, [0306] (Weiser describes "***SDCCH sub-channels***" for "carry[ing] control, ***SMS*** and Wireless Applications Protocol (WAP) traffic").



SAMSUNG-1006, FIG. 1 (annotated).

It would have therefore been obvious to utilize such well-known control channels for delivering control information included in the special SMS message and this would have amounted to implementing known methods/techniques (using a dedicated control channel, as per Minborg and Weiser) to known systems/devices (e.g., SDD's mobile devices) to achieve predictable results (transmission of control information in the special SMS message, per DB). SAMSUNG-1003, ¶212; SAMSUNG-1020, [0005]; SAMSUNG-1021, [0306]. Using such a dedicated control channel would have the additional benefit of reducing traffic on data channels.

SAMSUNG-1003, ¶212. A POSITA would have had a reasonable expectation of success in implementing a dedicated control channel for delivering special SMS messages given (1) common use of control channels for delivering control information and (2) well-known dedicated control channels that are regularly used in cellular network communications for transmission of the type of SMS messages (as DB teaches). SAMSUNG-1003, ¶212.

SDD further renders obvious that the control channel includes a connection from the secure modem subsystem to the control centre (i.e., a network service controller) and this channel is secure. SAMSUNG-1003, ¶213. Per Schmidt, TSS-DM (part of SDD's secure modem subsystem) "controls all internal and external communications and ***secures the communications channel***"—i.e., secures the above-described control channel. SAMSUNG-1005, [0032]; SAMSUNG-1003, ¶213; SAMSUNG-1058, 2.

Additionally, as described further in [1.4], SDD's control channels further include a connection between the SDD's SEE and the secure modem subsystem. SAMSUNG-1003, ¶214; SAMSUNG-1058. Thus, data for the first and second control channels pass from the SEE (including TSS-MNO) to the network service controller (control centre) via the secure modem subsystem (including TSS-DM). SAMSUNG-1003, ¶214. In other words, each of the first and second control channels includes (1) an internal connection from the TSS-MNO to the TSS-DM and (2)

an external connection from TSS-DM (and via the modem's transceiver circuitry) to the control centre—which together form the respective control channels (as further described with reference to [1.4] below). SAMSUNG-1003, ¶214. As Dr. McDaniel explains, it was common in networked systems for communication between certain on-device applications and external components to traverse intermediate components, e.g., the modem. SAMSUNG-1003, ¶214, §X.A.[1.4]. Thus, in view of the above, it would have been obvious for the above-described first secure control channel to provide a connection from the secure modem subsystem to a network service controller. SAMSUNG-1003, ¶214.

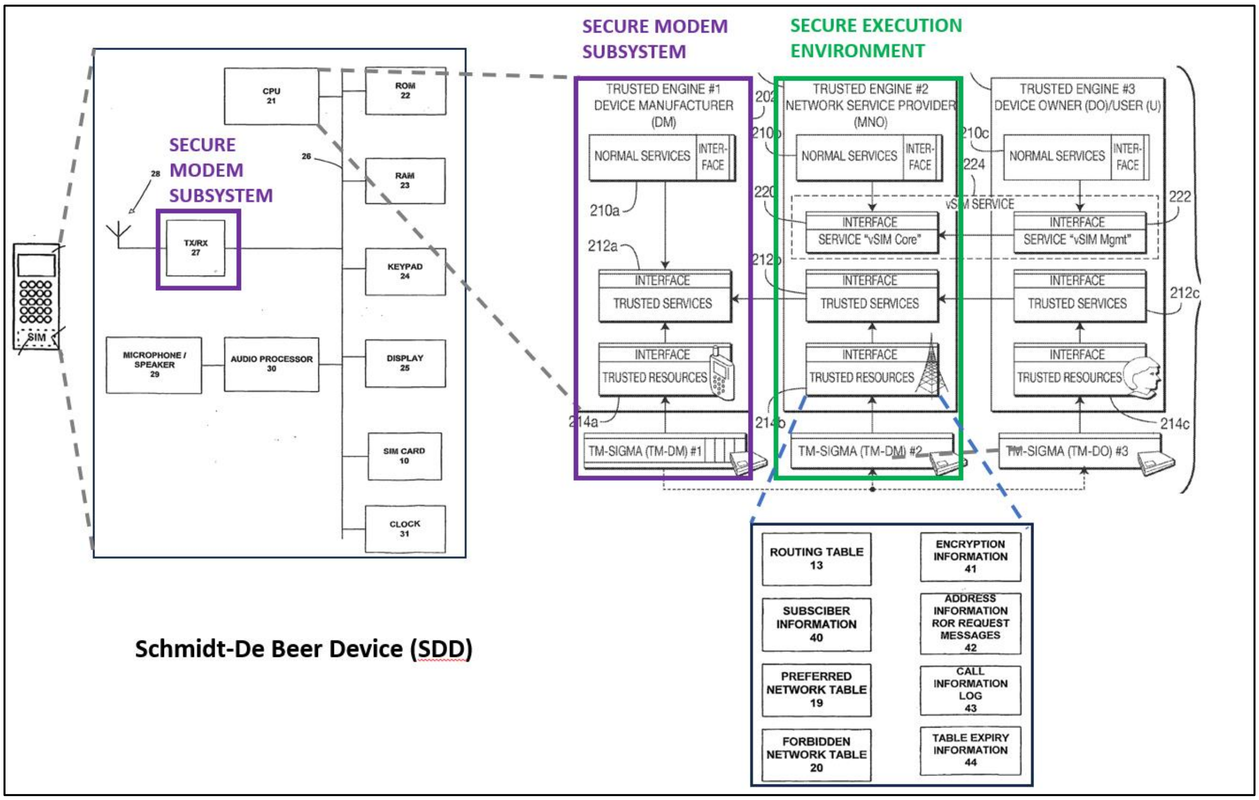
[1.4]

As explained below, SDD renders obvious connecting a second secure control channel (e.g., a channel established at a later time, over which an encrypted SMS message is sent) from a SEE (e.g., TSS-MNO/TM-SIGMA), separately secure from the secure modem subsystem, through the secure modem subsystem (e.g., TSS-DM with TX/RX) and the wireless cellular network (e.g., local network) to the network service controller (e.g., control centre). SAMSUNG-1003, ¶¶215-233.

SDD's MTP includes multiple TSSs, including TSS-MNO, which is included in a SEE. SAMSUNG-1003, ¶216. Per Schmidt, each TSS includes a "***trusted execution environment*** (TE-sigma) and the non-exchangeable security module

(trusted module, TM)." SAMSUNG-1005, [0031]. Each TSS is also "configured to sign and ***encrypt any given data.***" *Id.*

Additionally, TSS-MNO is a trusted subsystem/execution environment that manages and protects "the subscriber-related portion of the vSIM credential, and performs the client-side network authentication of a subscriber." SAMSUNG-1005, [0033]; SAMSUNG-1003, ¶217.



SAMSUNG-1005, FIG. 2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified), SAMSUNG-1003, ¶217.

SDD connects a second secure control channel to the network services controller. SAMSUNG-1003, ¶218. As explained in §III.A.3.e and [1.3] above, SDD

leverages DB's teachings of obtaining updated lookup tables from the control centre. SAMSUNG-1003, ¶218. Per DB, if a device lacks a soft reset facility, "the application must rely upon initiating re-registration ***when the user next turns off and on the power to the apparatus***." SAMSUNG-1006, [0065]. Therefore, when a user reboots the phone (in the same location), the registration process repeats—thus resulting in the connection of a second channel. SAMSUNG-1003, ¶218 ("[o]ne channel may be distinguished from other channels by the ***time of occurrence*** of the transmission"); SAMSUNG-1022, 3; SAMSUNG-1064, 101.

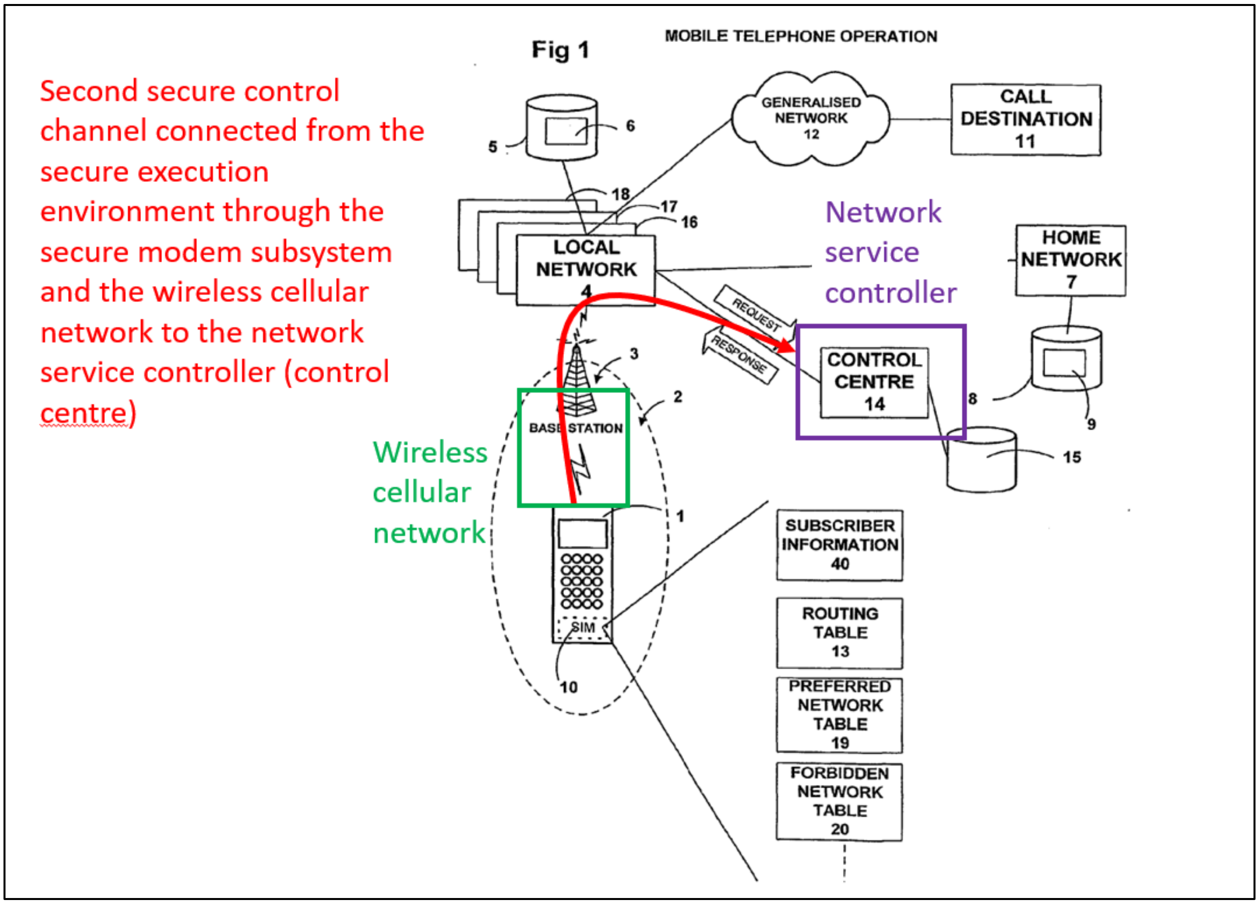
During registration, SDD determines whether the routing table is "still valid by comparing current date and time ... with an expiry date field included in the routing table." SAMSUNG-1006, [0050], [0072]. If "the routing table has expired," "a ***request message is generated… for an update of the routing table***." SAMSUNG-1006, [0072].

The "request message is transmitted as an SMS message to the control centre which sends a response message in SMS format" that includes the updated routing table 13. SAMSUNG-1006, [0072].

As explained above in [1.3], a POSITA would understand or find obvious that the SMS message from SDD includes control information and would be sent over a control channel (e.g., a dedicated channel such as a SDCCH). SAMSUNG-1003, ¶221, §III.A.4.[1.3].

The claim does not specify that the "first control channel" is distinct from the "second control channel." Nevertheless, if interpreted as such, a POSITA would recognize or find obvious that the control channel used for transmission of the above-described control information would be a separate channel from the first control channel, as described above for element [1.3]. SAMSUNG-1003, ¶222.

As Dr. McDaniel explains, the second control channel is at least temporally distinct (e.g., existing on a different day) from the first control channel. SAMSUNG-1003, ¶¶223-224; SAMSUNG-1022, 3. Additionally, or alternatively, a POSITA would recognize or find obvious that this control channel would be physically or logically distinct from the above-identified "first control channel." As explained for [1.3], a dedicated control channel (e.g., SDCCH) may be used for sending and receiving the above-described information. Such dedicated channels are released and/or torn down after their use, such that, at a later time, a new dedicated channel—with updated channel properties—is connected. SAMSUNG-1003, ¶225, §III.A.4.[1.3]. Therefore, a POSITA would understand or find obvious that, when SDD is powered off (e.g., overnight) and subsequently restarted in the same location, SDD will connect through the same local network (wireless cellular network) via a second secure control channel to the control centre (network service controller) to obtain updated tables. SAMSUNG-1003, ¶225.



SAMSUNG-1006, FIG. 1 (annotated).

Additionally, SDD connects the above-described second secure control channel to the network service controller from the SEE. SAMSUNG-1003, ¶226. SDD's registration process includes a connection from TSS-MNO because, per Schmidt, "[a]ll subscription-dependent and subscriber-related network provider services of a platform are allocated to the TSS-MNO." SAMSUNG-1005, [0033]. A POSITA would recognize that the above-described registration process which occurs while the device is roaming—per DB—is both subscription-dependent and subscriber-related. SAMSUNG-1005, [0033]; SAMSUNG-1003, ¶226; SAMSUNG-

1038, [0002]. Therefore, in SDD's architecture, the connection of the second control channel would be from SDD's SEE (TSS-MNO/TM-SIGMA), via the secure modem subsystem (since its TSS-DM component "controls all internal and external communications"), to the network service controller (control centre). SAMSUNG-1005, [0032]; SAMSUNG-1003, ¶¶226-231.

As with the first secure control channel described above, this second control channel is also secure because (1) per Schmidt, TSS-MNO encrypts communications it sends and (2) TSS-DM (part of the secure modem subsystem) "controls all internal and external communications"—such as the communication channel including the second control channel—and "***secures [this] communications channel***." SAMSUNG-1005, [0032]; §III.A.4.[1.3].

Finally, SDD's SEE (TSS-MNO/TM-SIGMA) is separately secure from the secure modem subsystem (including SDD's transceiver circuitry operating with TSS-DM). SAMSUNG-1003, ¶233. Per Schmidt, the device includes "three ***separate*** trusted" subsystems and "multiple protected***, separate*** execution environments." SAMSUNG-1005, [0028], [0030]. Therefore, SDD's SEE (TSS-MNO/TM-SIGMA) is separate from the secure modem subsystem (which includes TSS-DM). SAMSUNG-1003, ¶233. Further, they are separately secure because ***each*** is a separate secure/trusted executed environment and "is [also] configured to sign and encrypt any given data." SAMSUNG-1005, [0031]; SAMSUNG-1003,

¶233.

[1.5]

As explained below, SDD renders obvious receiving at the SEE (e.g., TSS-MNO/TM-SIGMA), via the second secure control channel, one or more messages comprising one or more service policy settings (e.g., a response message including routing table updates) from the network service controller (e.g., control centre). SAMSUNG-1003, ¶¶234-238.

As described in [1.4], when the routing table has expired, SDD transmits a "request message … as an SMS message to the control centre," which "responds by retrieving data from its database" and "transmitting a response message in SMS format." SAMSUNG-1006, [0072]. The response message includes an updated routing table, which is used to update SDD's existing routing table. SAMSUNG-1006, [0073]; SAMSUNG-1003, ¶235.

A POSITA understands or finds obvious that the request and response messages, which are both SMS messages, would use the same control channel. SAMSUNG-1003, ¶236 ("where a request and response are sent in quick succession, it is resource efficient to use the same channel for both… messages.").

The "routing information" includes service policy settings such as "routing table 13, preferred network table 19 and forbidden network table 20." SAMSUNG-1006, [0055]; SAMSUNG-1003, ¶237. A POSITA understands that the data in these

tables are policy settings because they constrain the device's use of the network. SAMSUNG-1003, ¶237; SAMSUNG-1036, 1; SAMSUNG-1057, 2; *see also* [8]-[9] (further describing how these are policy settings).

Further, since the routing information is subscription and subscriber dependent, and "[a]ll subscription-dependent and subscriber-related network provider services … are allocated to the TSS-MNO" (per Schmidt), a POSITA would understand or find obvious that the policy settings in SDD would be received by TSS-MNO, and therefore by the SEE (of which TSS-MNO is a component). SAMSUNG-1005, [0033]; SAMSUNG-1003, ¶238.

[1.6]

As explained below, SDD renders obvious storing the service policy settings (e.g., updated routing table entries received from the control centre) in a secure memory partition accessible only from the SEE (e.g., TSS-MNO/TM-SIGMA). SAMSUNG-1003, ¶¶239-245.

As explained in §§III.A.3.d-e, SDD includes a secure memory partition in its on-device memory and stores therein lookup tables including routing information (which are policy settings). *See* SAMSUNG-1006, [0046], [0067], FIG. 4; SAMSUNG-1003, ¶240; [1.5].

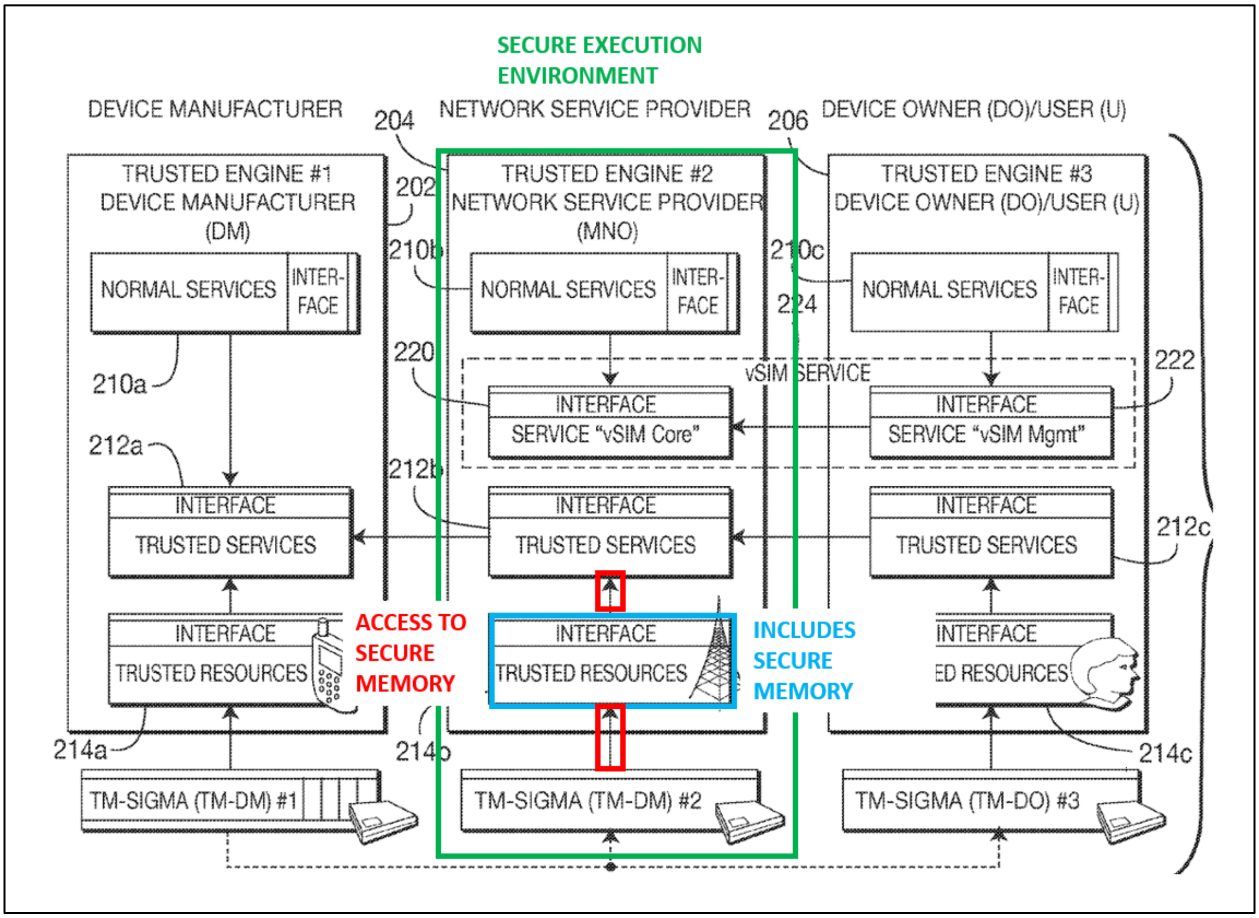
Additionally, per DB and as explained in §§III.A.3.d-e, when SDD receives

the updated routing information (i.e., service policy settings), it stores/updates this information in the secure memory partition. SAMSUNG-1003, ¶240. Per DB, when the mobile terminal requests updated routing information (*see* analysis for [1.4] *supra*), the control centre responds by transmitting "up-to-date tables from its database" in "a response message via the local network" to the device, where the existing tables "***are updated with the received data***." SAMSUNG-1006, [0046], [0067], FIG. 4. Because SDD includes a secure memory partition (where this information is stored (*see* §III.A.3.d)), a POSITA would understand or find obvious that the lookup tables stored in this secure memory partition, are updated and stored therein using the received updated information. SAMSUNG-1003, ¶241.

Further, a POSITA would understand or find obvious that SDD's policy settings (e.g., routing table, preferred network table, forbidden network table) stored in the secure memory partition are accessible only from the SEE (TSS-MNO/TM-SIGMA). SAMSUNG-1003, ¶242. As Schmidt explains, "TSS-MNO includes a vSIM core services unit, configured to ***store***, provide and process credential information" and this vSIM core "perform[s] the SIM functions related to the MNO." SAMSUNG-1005, [0005], [0029]. TSS-MNO further "is responsible for managing and ***protecting the subscriber-related portion of the vSIM credential.***" SAMSUNG-1005, [0033]. Additionally, Schmidt discloses that each TSS, including TSS-MNO, has its own dedicated set of trusted resources—which a POSITA would

understand or find obvious as including trusted/secure storage. SAMSUNG-1003, ¶¶242-244; SAMSUNG-1030, 28.

The trusted resources (including trusted storage) of TSS-MNO are accessible only from the trusted resources interface in TSS-MNO (part of the SEE). SAMSUNG-1003, ¶245. For example, Schmidt's FIG. 2 demonstrates that the TSS-MNO's trusted resources (which include secure memory) are available only through the "interface" to the "trusted resources" within TSS-MNO, accessible by "trusted services" and the "trusted entity of the security module." SAMSUNG-1005, FIG. 2, [0028], [0037]; SAMSUNG-1003, ¶245. Additionally, given Schmidt's explanation that each TSS is separate and isolated from other TSSs, a POSITA would understand or find obvious that the trusted resources of a particular TSS, such as TSS-MNO, would be accessible by TSS-MNO and not by any other TSS or system component. SAMSUNG-1003, ¶245.



SAMSUNG-1005, FIG. 2 (annotated).

[1.7]

As explained below, SDD renders obvious enforcing, at least in part from the SEE (e.g., TSS-MNO/TM-SIGMA), a network service profile (e.g., data files) comprising the one or more service policy settings (e.g., routing table, preferred network table, forbidden network table), to control wireless end-user device use of a service on the wireless cellular network (e.g., voice and/or data use on the local network and

generalized networks). SAMSUNG-1003, ¶¶246-258.

The ’429 specification does not define “network service profile.” A POSITA would understand that a network service profile includes a collection of information used to control the “interactions between the mobile telephone and the current network.” SAMSUNG-1003, ¶247; SAMSUNG-1037, Abstract. Consistent with this understanding, the policy settings stored in SDD’s secure memory partition (e.g., routing table, preferred network table, forbidden network table, as explained in §III.A.3.d, [1.5]-[1.6]) would be understood as a network service profile because they represent a collection of information that is used to control the interactions between the mobile telephone and the network (e.g., network access and call routing over the network). SAMSUNG-1006, [0033]-[0034], [0036]; SAMSUNG-1003, ¶247.

Additionally, and consistent with the ’429 specification, a POSITA would recognize or find obvious that the policy settings stored in SDD’s secure memory partition (e.g., routing table, preferred network table, forbidden network table, per §III.A.3.d, [1.5]-[1.6]) are included in, or associated with, a network service profile. SAMSUNG-1006, [0046], FIG. 4; SAMSUNG-1003, ¶248; SAMSUNG-1001, Abstract.

For example, DB explains that the routing table is used to choose a call route with minimum cost, such that call routing and cost for completing a call, provide

access to a service (e.g., voice calling) on a service plan. SAMSUNG-1006, Abstract, [0034], [0097]-[0098]; SAMSUNG-1003, ¶249; *see* analysis for [2] (explaining that network service profile including its policy settings are associated with a service plan).

Additionally, per DB, the forbidden network table "lists those networks for which the subscriber ***does not have authorisation*** from the home network" to complete registration. SAMSUNG-1006, [0036]. A POSITA would recognize that such authorization to access (or not) a network is also related to the service plan since it enables access to a network and its services. SAMSUNG-1003, ¶¶250-251; SAMSUNG-1038, [0002]. Similarly, DB explains that, in "selecting a network for registration purposes," the device "refers to a preferred network table 19 which lists networks in order of preference." SAMSUNG-1006, [0036]. This "list of available networks is compared with the" networks listed in the "preferred network table," and if one or more networks "in the available network list is found in the preferred network table," the preferred network is "***selected for registration***." SAMSUNG-1006, [0058].

As explained below, SDD's SEE (TSS-MNO/TM-SIGMA) enforces, at least in part, the network service profile to control the device's use of a service on the wireless cellular network. SAMSUNG-1003, ¶252. For example, per DB, SDD enforces call routing to a call destination using at least the updated routing table

(policy setting in the network service profile), thereby controlling the use of a voice service on the wireless cellular network. SAMSUNG-1003, ¶¶252; SAMSUNG-1006, [0032]. Per DB, when the device initiates a call, it "has ***a call routing facility***" that "allows routing information [stored in the tables] to be accessed" and "added to a user defined call number." SAMSUNG-1006, [0032]-[0033]. In this manner, "a setup procedure initiated via the local network" results in the connection path to the call destination "being ***determined in accordance with a preferred route***." SAMSUNG-1006, [0032].

Additionally, per DB, the "preferred network table [] lists networks in order of preference" and the forbidden network table lists "those networks for which the subscriber does not have authorisation from the home network" "to complete registration." SAMSUNG-1006, [0036]; SAMSUNG-1003, ¶253. As explained above, the preferred network table is enforced by the device, which determines "[i]f one or more of the MNCs in the available network list is found in the preferred network table", the preferred network is "***selected for registration***." SAMSUNG-1006, [0058]; SAMSUNG-1003, ¶253. The forbidden network table is enforced at the device which compares "each network in the list [of available networks] with the forbidden network table" and "any networks which are excluded are removed from the list of available networks." SAMSUNG-1006, [0057]; SAMSUNG-1003, ¶253.

Further, DB explains that when "the country code is new," then "a request

message must be generated in order to obtain new versions" of the routing table, preferred network table and the forbidden network table. SAMSUNG-1006, [0067]. Then the "local network [the wireless cellular network] with which the mobile telephone is now registered" is compared with the updated preferred network table and forbidden network table, and if "another one of the available networks has a higher level of preference in the list, a process of re-registration is initiated ... to replace the currently registered network with the preferred network which then becomes the 'local network'." SAMSUNG-1006, [0068]. Per DB, if the currently registered network is listed in the forbidden network table, then DB forces re-registration. SAMSUNG-1006, [0069]. Thus, SDD enforces service policies to control SDD use of the local network, e.g., by dropping access to the local network (disallowing access to the service over the local network) if the local network is forbidden or not preferred. SAMSUNG-1003, ¶254.

Because SDD leverages the above teachings in DB, the routing information, preferred network table and forbidden network table are used by SDD to enforce policies used to control the wireless end-user device use of a network service (e.g., telephony, data), e.g., by selecting a least-cost route, using a preferred network and/or avoiding forbidden networks. SAMSUNG-1003, ¶255. Thus, SDD enforces service policies to control SDD use of the local network ["the wireless cellular network"], e.g., by determining routing over the network. SAMSUNG-1003, ¶255.

In DB, routing is performed by the SIM processor. SAMSUNG-1006, [0052]-[0053]; SAMSUNG-1003, ¶256. Since SDD has no physical SIM, such processes, when implemented in SDD, would be performed by SDD's trusted services. SAMSUNG-1003, ¶256. In particular, and as explained in [1.5], the routing information, preferred network table and forbidden network table are subscription and subscriber dependent. SAMSUNG-1003, ¶257. Because all such services "are allocated to the TSS-MNO," a POSITA would have been motivated and would have had reason to implement policy enforcement in SDD, at least in part, by the TSS-MNO (part of the SEE). SAMSUNG-1005, [0033]; SAMSUNG-1003, ¶257. Indeed, such an implementation, which would be straightforward to implement (in view of DB's disclosures) and amounts to implementing of known techniques to a known system to achieve predictable results—ensuring that the security benefits provided by a SIM processor are maintained in the context of the SDD vSIM architecture, where the trusted services, including those of TSS-MNO, provide the same security benefits. SAMSUNG-1003, ¶257.

In summary, Schmidt teaches that the SEE (TSS-MNO/TM-SIGMA) is responsible for "managing and protecting" the vSIM data (including the network service profile) and "performs the SIM functions related to the MNO." SAMSUNG-1005, [0033]. In view of Schmidt and DB, a POSITA would thus understand or find obvious that the TSS-MNO (a component of the SEE) would access the stored policy

settings (since only TSS-MNO has access to the data) from its dedicated memory partition and would be the entity responsible, at least in part, for the above-described enforcement of the network constraints defined by this data, e.g., network access and least cost call routing. SAMSUNG-1003, ¶258.

[2]

SDD renders obvious that the network service profile is associated with a service plan that provides for access to the service on the wireless cellular network. SAMSUNG-1003, ¶¶259-262.

The '429 specification does not define a "service plan." SAMSUNG-1001. A POSITA would understand that a service plan "can provide data services, voice services or a combination of voice and data services" and can define pricing for these services. SAMSUNG-1003, ¶260; SAMSUNG-1038, [0002].

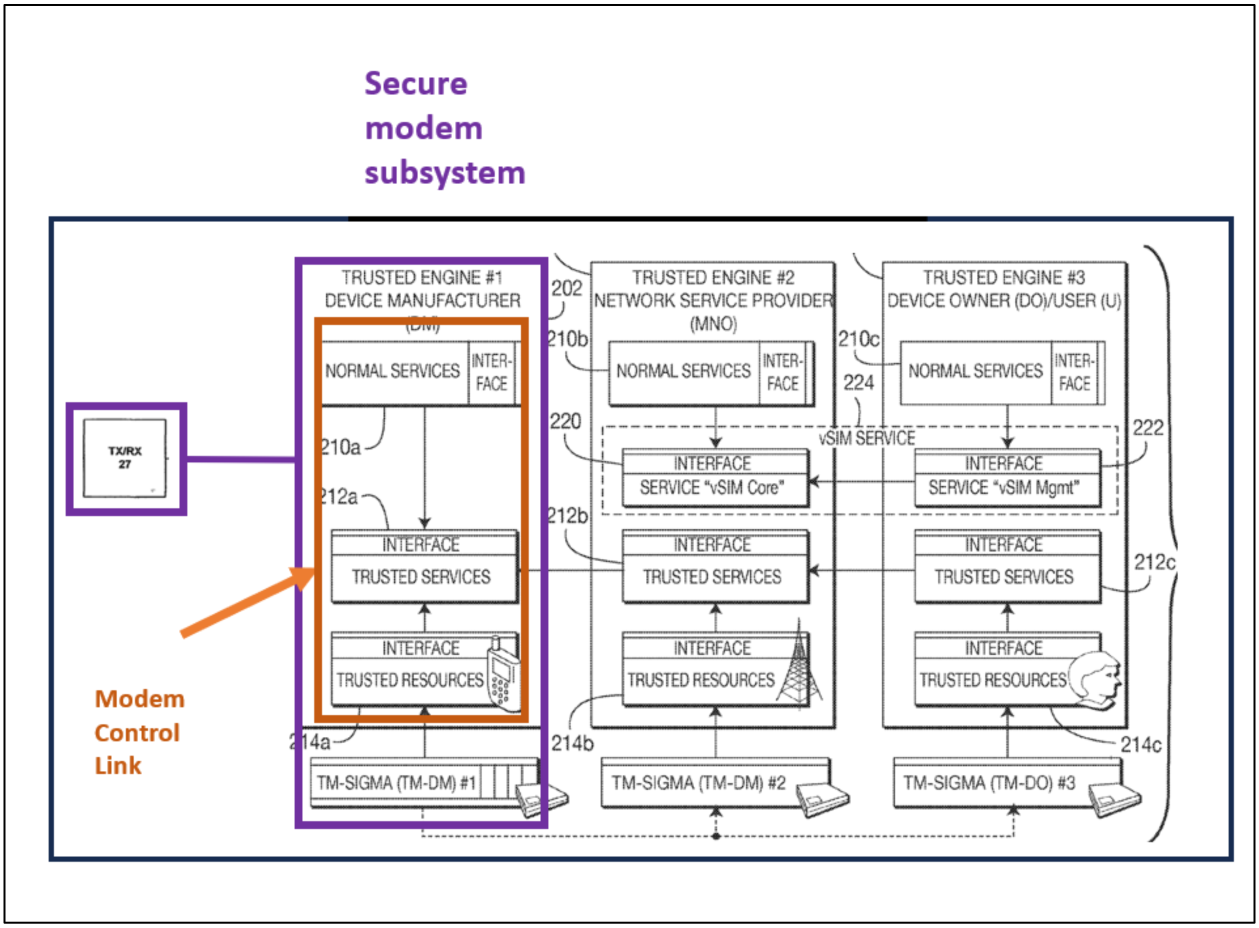
Consistent with this understanding, and based on DB's teachings, SDD's device subscribes to a service plan that provides access to services (e.g., voice, data services) and uses stored policy settings to facilitate such service access. SAMSUNG-1003, ¶261; *see* [1.5]-[1.7] *supra*. Per DB, a home network "is operated by a home service provider with whom a subscriber using the mobile telephone" has "***a contractual relationship***." SAMSUNG-1006, [0030]. Per DB, the routing table is used to choose a call route with minimum cost, such that call routing and cost for completing a call provide access to a service (e.g., voice calling) on a service plan

(with associated cost for use of such service). SAMSUNG-1006, Abstract, [0034], [0097]-[0098]; SAMSUNG-1003, ¶261. Additionally, the forbidden network table "lists those networks for which the subscriber ***does not have authorisation*** from the home network" to complete registration. SAMSUNG-1006, [0036]. From these disclosures, a POSITA would recognize that such authorization relates to accessing a network and by extension, relates to the service plan. SAMSUNG-1003, ¶261.

Moreover, as explained in [1.7], SDD includes a network service profile that includes policy settings. Because the device subscribes to a service plan and uses the same policy settings to control access to the plan's services (as described in [1.7]), a POSITA would understand that SDD's network service profile (and associated policy settings) is associated with a service plan that provides access to services (e.g., voice calling, data services) on the wireless cellular network. SAMSUNG-1003, ¶262.

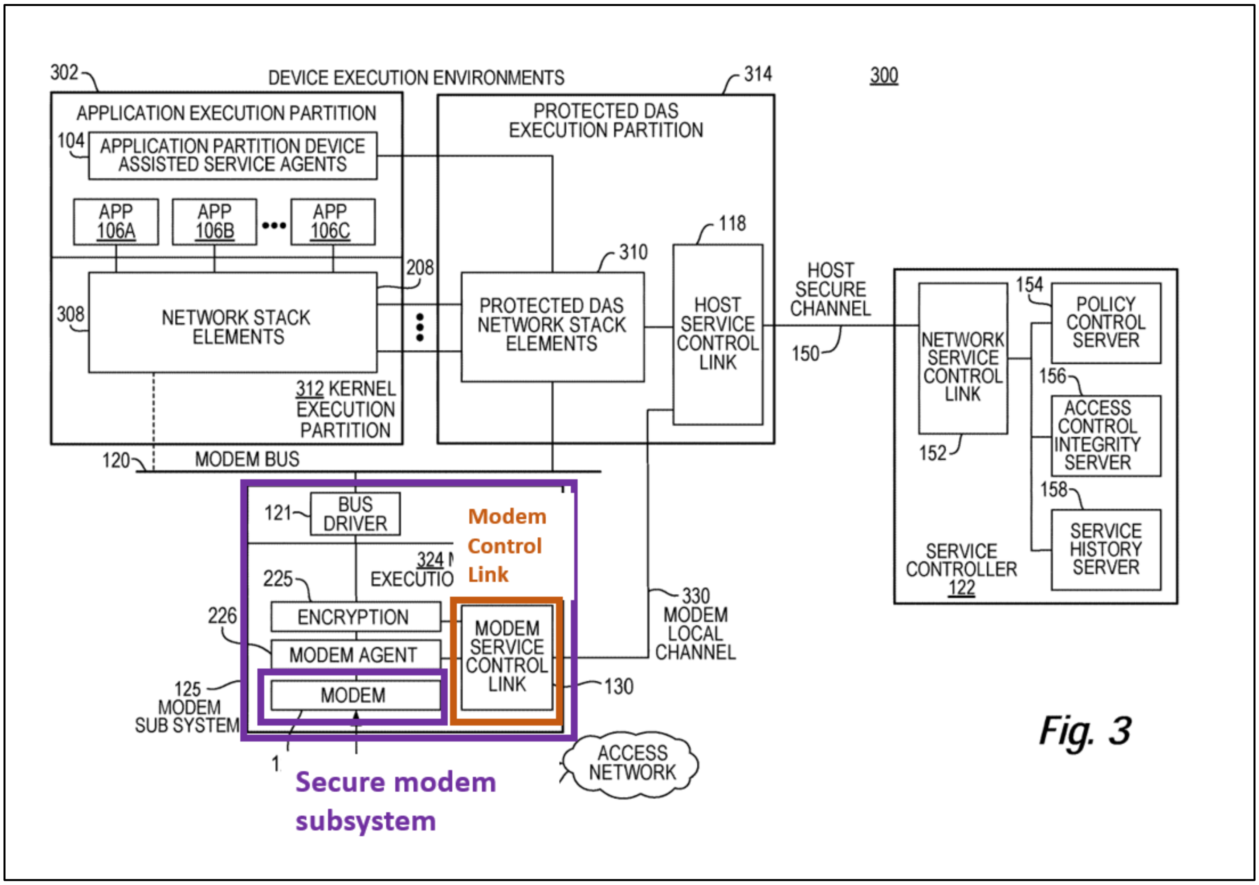
[3.1]

As shown below, SDD's secure modem subsystem comprises a modem control link coupled to the physical modem (TX/RX) in the secure modem subsystem. SAMSUNG-1005, [0032]; SAMSUNG-1006, [0042]; SAMSUNG-1003, ¶¶263-267.



SAMSUNG-1005, FIG. 2 (excerpts, annotated); SAMSUNG-1006, FIG. 2 (excerpts, annotated); SAMSUNG-1003, ¶¶263-264.

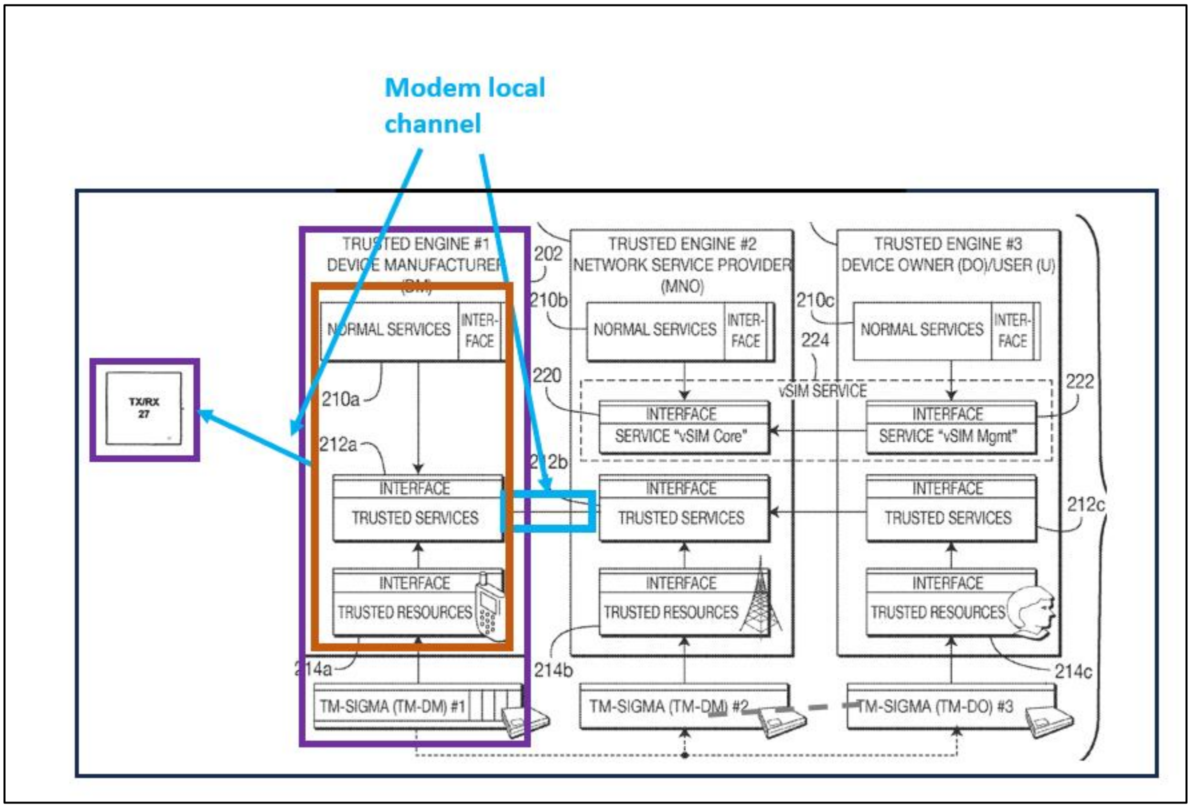
This structure is analogous to the '429 Patent's FIG. 3 embodiment (reproduced below) in which the modem control link ("modem service control link") and the physical modem ("modem") are components of the modem subsystem. SAMSUNG-1001, 10:29-48; SAMSUNG-1003, ¶264.



SAMSUNG-1001, FIG. 3 (annotated).

As shown below, SDD's secure modem subsystem further comprises a modem local channel that couples the modem control link to TSS-MNO and TX/RX – that is, components that are ***local*** to the device. SAMSUNG-1003, ¶265. A POSITA would understand that the modem subsystem includes this modem local channel since TSS-DM "controls all internal and external communications and secures the communications channel," and therefore interchanges data both with TSS-MNO, which is allocated "[a]ll subscription-dependent and subscriber-related network provider services," and the TX/RX, the hardware used to send/receive cellular data.

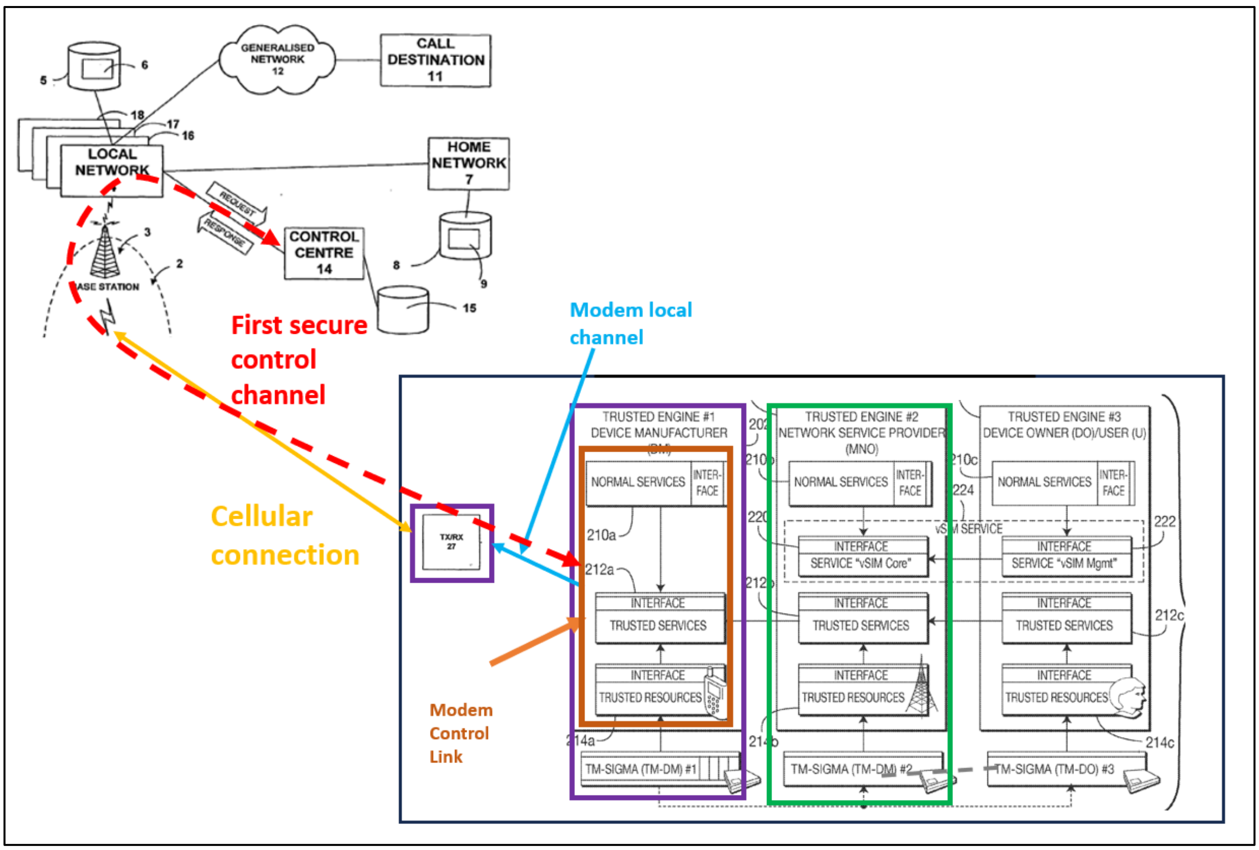
SAMSUNG-1005, [0032]-[0033]; SAMSUNG-1006, [0042]; SAMSUNG-1003, ¶266.



SAMSUNG-1005, FIG. 2 (excerpts, annotated); SAMSUNG-1006, FIG. 2 (excerpts, annotated); SAMSUNG-1003, ¶266.

Additionally, the first secure control channel connects the modem control link to the network service controller through the modem local channel. SAMSUNG-1003, ¶267; *see* SAMSUNG-1001, FIG. 3 and associated description (describing similar functionality). As described in [1.3]-[1.6], control channels facilitate transmission of policy settings (and requests for the same) between the secure modem subsystem (which includes the transceiver circuitry and TSS-DM) and the network

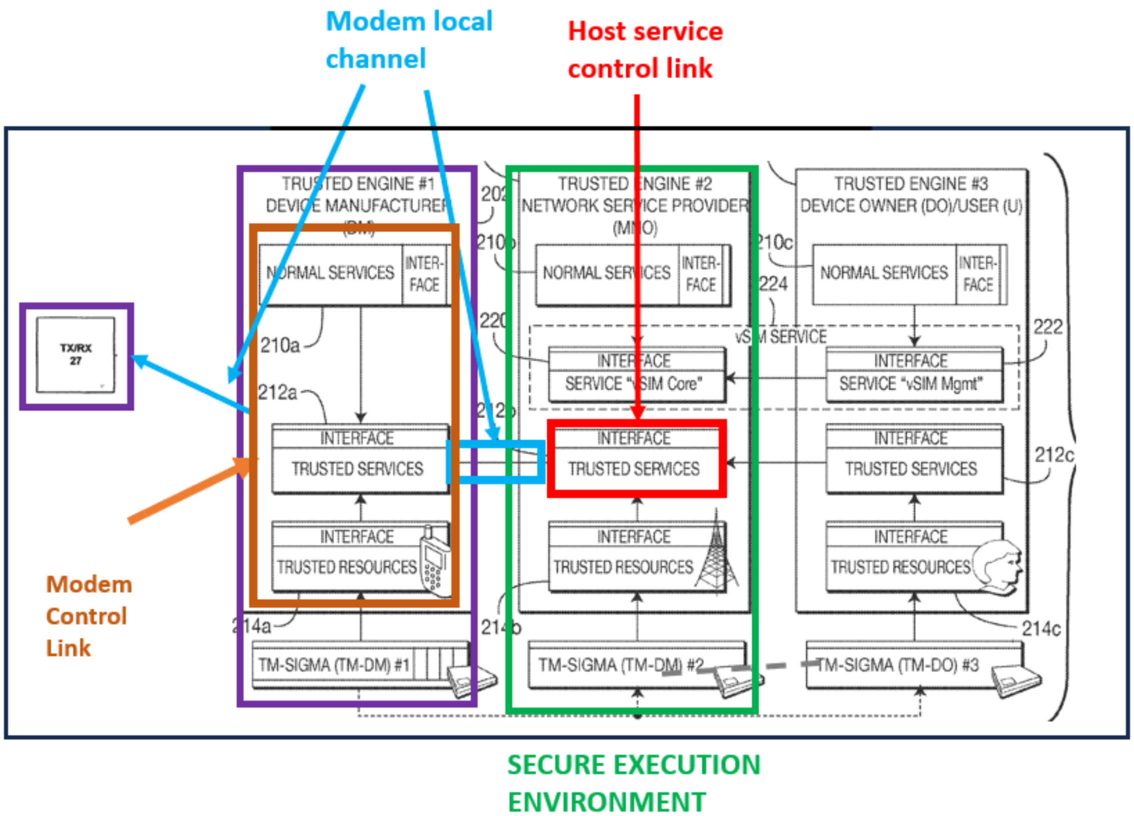
service controller (control centre). It follows that this control channel connects the modem control link (in TSS-DM, which controls all communication of SDD) to/from the network service controller (i.e., control centre) and such a connection would be via the modem local channel that connects the modem control link to the transceiver (TX/RX) circuitry, as described above. SAMSUNG-1005, [0032]; SAMSUNG-1006, [0042]; SAMSUNG-1003, ¶267.



SAMSUNG-1005, FIGS. 2 (excerpts, annotated); SAMSUNG-1006, FIGS. 1, 2 (excerpts, annotated); SAMSUNG-1003, ¶267.

[3.2]

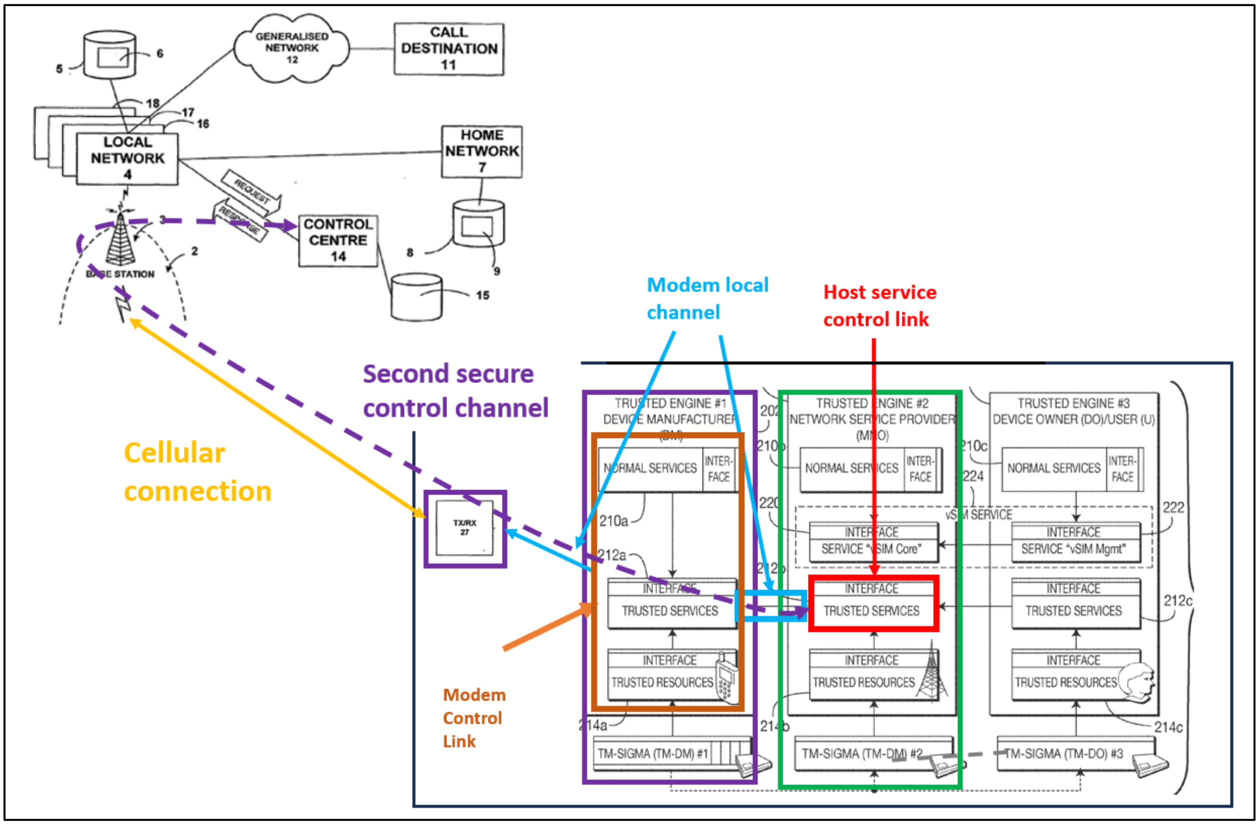
In SDD, the SEE (TSS-MNO/TM-SIGMA) comprises a host service control link that "facilitates communication with a host secure channel." SAMSUNG-1001, 6:9-11; §III.A.3; SAMSUNG-1003, ¶¶268-270. As illustrated in Schmidt's FIG. 2, TSS-MNO's trusted services interface (host service control link) couples TSS-MNO and TSS-DM, and since TSS-DM controls all external communication, a POSITA would understand that TSS-MNO's trusted services interface facilitates communication with the secure control channels (via TSS-DM to the control centre, e.g., to retrieve policy settings). SAMSUNG-1005, FIG. 2, [0032]; *see* [1.4]-[1.6]; SAMSUNG-1003, ¶268.



SAMSUNG-1005, FIG. 2 (annotated); SAMSUNG-1006, FIG. 2 (excerpt); SAMSUNG-1003, ¶268.

In SDD, the second secure control channel is coupled to the host service control link. SAMSUNG-1003, ¶269. As explained in [1.4]-[1.6], SDD's TSS-MNO facilitates communication to the control centre (network service controller), e.g., to retrieve policy settings over the first and second secure control channels. SAMSUNG-1005, [0033]; *see* [1.4]-[1.6]; SAMSUNG-1003, ¶269. Because TSS-MNO's trusted services interface (host service control link) couples TSS-MNO and

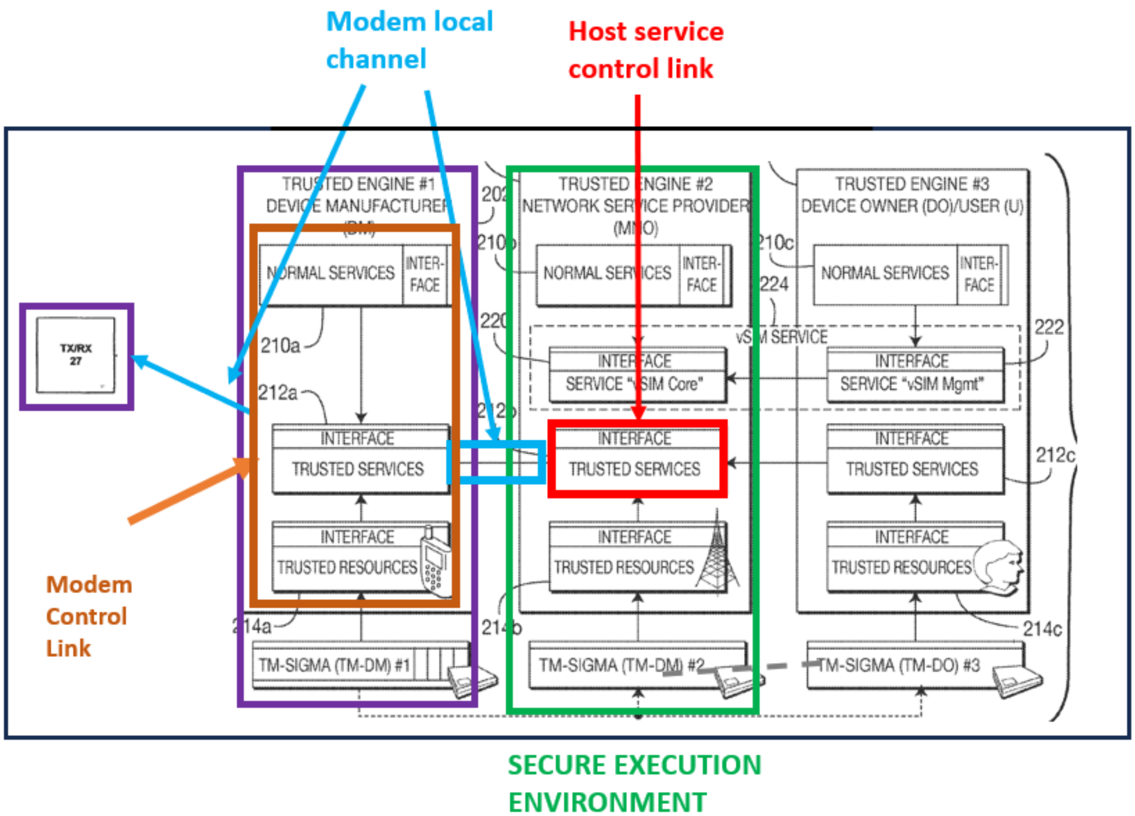
TSS-DM, and TSS-DM controls all external communication, the second secure control channel is coupled to the host service control link. SAMSUNG-1005, [0032]; SAMSUNG-1003, ¶269.



SAMSUNG-1005, FIG. 2 (annotated); SAMSUNG-1006, FIGS. 1, 2 (annotated); SAMSUNG-1003, ¶269.

In SDD, as illustrated below, the modem local channel provides secure communication between the modem control link (e.g., in TSS-DM) and the host service control link (TSS-MNO's trusted services interface). SAMSUNG-1003, ¶270. Since each "TSS-sigma is always configured to sign and encrypt any given data," a POSITA would understand that communication between the modem control link and

the host service control link is secure (encrypted). SAMSUNG-1005, [0031]; SAMSUNG-1003, ¶270.



SAMSUNG-1005, FIG. 2 (annotated); SAMSUNG-1006, FIG. 2 (excerpt, annotated).

[8]

SDD's service policy settings (described above in [1]) include traffic control settings. SAMSUNG-1003, ¶¶271-273. In SDD, the routing table specifies traffic control settings for determining a connection path to a call destination. SAMSUNG-1006, [0032]-[0033], [0087]; SAMSUNG-1003, ¶271. Per DB, "when an outgoing

call to a call destination" is initiated, the device "intercepts the call making process and provides a call output means 109 with ***routing information*** which will determine the route taken" through the generalised network between the local network and the call destination. SAMSUNG-1006, [0087]. Because the routing information controls how data traffic passes/is routed through the network, a POSITA would understand that the routing information is a traffic control setting. SAMSUNG-1003, ¶271.

Additionally, SDD's service policy settings include a forbidden network table used to enforce access control settings when selecting a network for registration. SAMSUNG-1006, [0036], [0046]; SAMSUNG-1003, ¶272. Per DB, "forbidden network table … lists those networks for which the subscriber does not have authorisation from the home network" to complete registration. SAMSUNG-1006, [0036]. Per DB, "any networks which are excluded are removed from the list of available networks." SAMSUNG-1006, [0057]. Therefore, in SDD, access to a forbidden network is controlled (disallowed) at the device (SDD) based on the forbidden network table (policy setting) and therefore, these service policy settings are access control settings. SAMSUNG-1006, [0036], [0057]; §III.A.3.e; SAMSUNG-1003, ¶273.

[9]

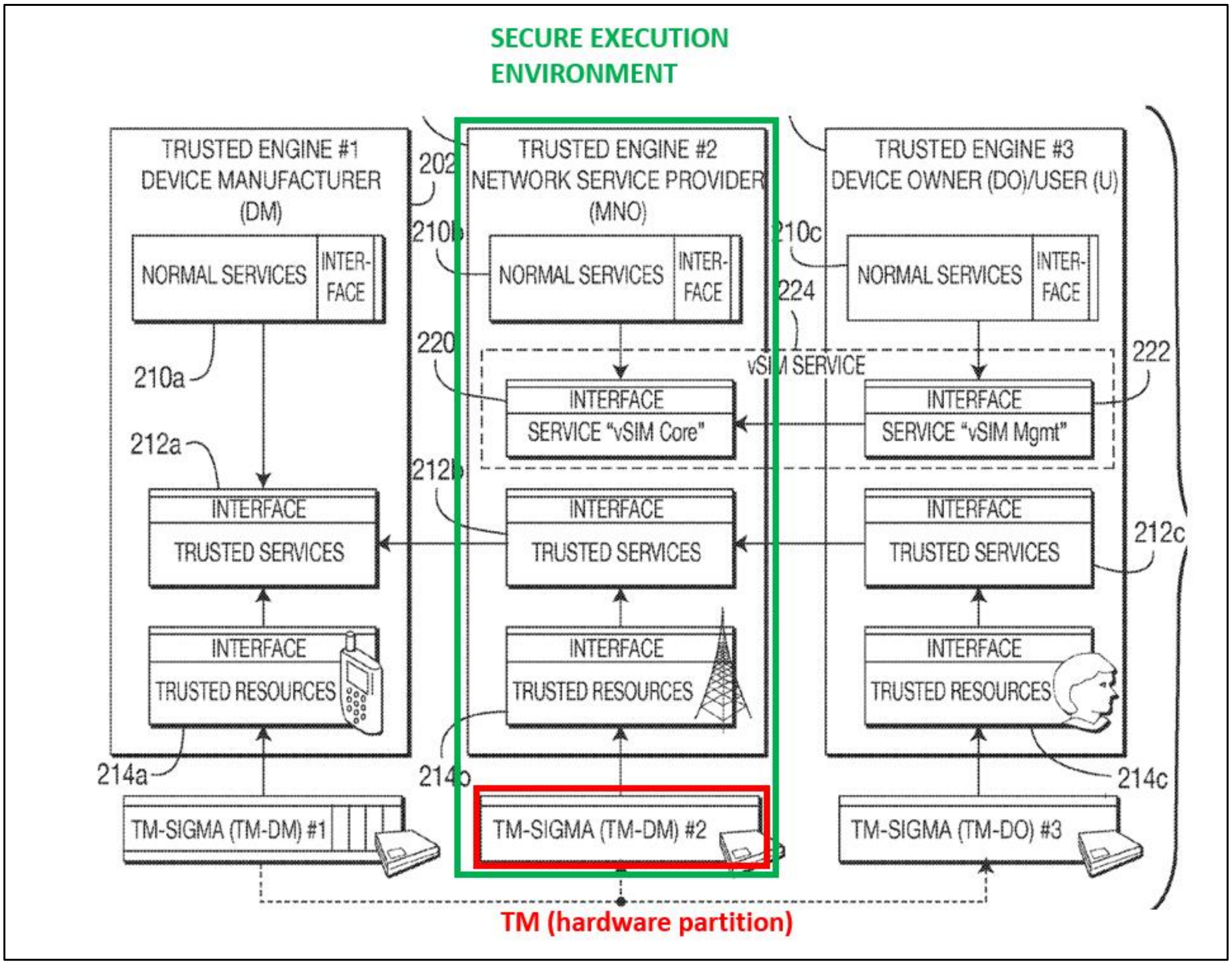
SDD's service policy settings include network management communication

settings. SAMSUNG-1003, ¶¶274-275. As explained for [8], SDD leverages DB's teachings of storing and using a routing table (network management communication setting) to determine a connection path to a call destination. SAMSUNG-1006, [0032]-[0033], [0087]; SAMSUNG-1003, ¶274. "[W]hen an outgoing call to a call destination 11 is initiated," the device "intercepts the call making process and provides a call output means 109 with ***routing information*** which will determine the route taken" through the network. SAMSUNG-1006, [0087].

A POSITA would understand or find obvious that determining a preferred route is a network management communication setting because it manages how the device communicates over the network, e.g., by defining a route. SAMSUNG-1003, ¶275.

[10]

A POSITA would understand or find obvious that SDD's SEE is implemented at least in part as a hardware partition. SAMSUNG-1003, ¶¶276-277; SAMSUNG-1049, 13; SAMSUNG-1054, 1-3. Per Schmidt, the MTP "is a mobile platform having a non-exchangeable security module (trusted module, TM) permanently associated with the ***hardware platform***." SAMSUNG-1005, [0036]. A POSITA would understand that TM is a hardware partition. SAMSUNG-1003, ¶276. Per Schmidt, SEE includes a TM (TM-SIGMA (TM-DM) #2). SAMSUNG-1005, [0031], [0037], FIG. 2; SAMSUNG-1003, ¶¶276-277.



SAMSUNG-1005, FIG. 2 (annotated).

[11]

In SDD, the SEE is implemented at least in part as a software partition. SAMSUNG-1003, ¶278. Per Schmidt, TSS-MNO (part of SEE) is implemented as one of multiple separate and isolated trusted subsystems—i.e., in separate partitions implemented in software—within MTP/device. *Id.*; SAMSUNG-1005, [0036], [0054].

[12]

Per Schmidt, the "MTP operates a trusted operating system," and the "trusted

software layer supports multiple separate trusted subsystems" (including TSS-MNO/TM-SIGMA) "with a protected and insulated execution and memory function"—which together would be understood as virtual machines (VMs). SAMSUNG-1005, [0036]; §III.A.3.f; SAMSUNG-1003, ¶¶279-280; SAMSUNG-1067. A POSITA would therefore recognize that SEE (TSS-MNO/TM-SIGMA) is executed at least in part on a VM. SAMSUNG-1003, ¶279.

Further, the above-described VM is executed at least in part on a processor. SAMSUNG-1003, ¶280. Per Schmidt, the MTP and associated trusted software layers of the TSSs (including SEE) would be implemented "in a computer-readable storage medium for ***execution by a general purpose computer or a processor***." SAMSUNG-1005, [0143]; SAMSUNG-1003, ¶280.

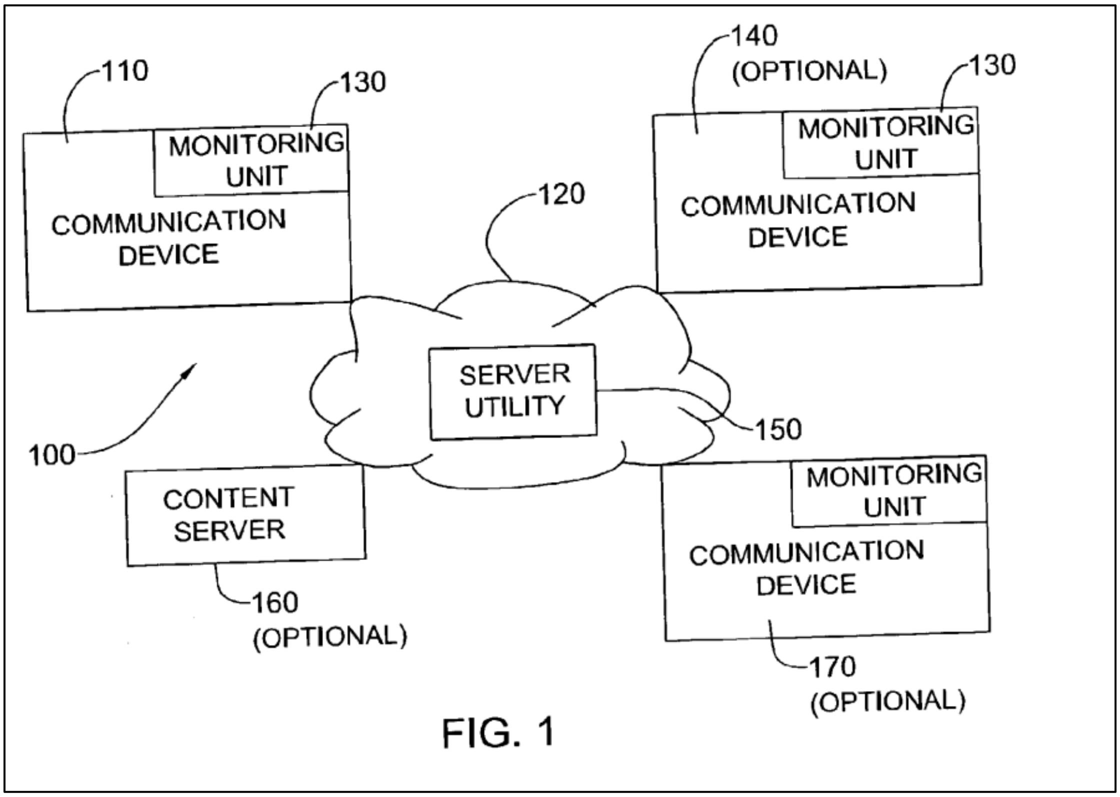
B. GROUND 1B – Schmidt-De Beer-Bittmann Renders Obvious Claims 4-7

1. Bittmann

Bittmann describes techniques for "real time management of a communication network account" associated with a mobile device. SAMSUNG-1007, Abstract.

Bittmann's system (below) provides a communication device that includes a monitoring unit that "monitors data activity of [a] communication device" and "manages the [device's] account." SAMSUNG-1007, Abstract, [0022]-[0023], [0028]-[0029]. The monitoring unit monitors the device's data activity, e.g., "web surfing,

game-playing, emails, short message service (sms)," etc. SAMSUNG-1007, [0031].



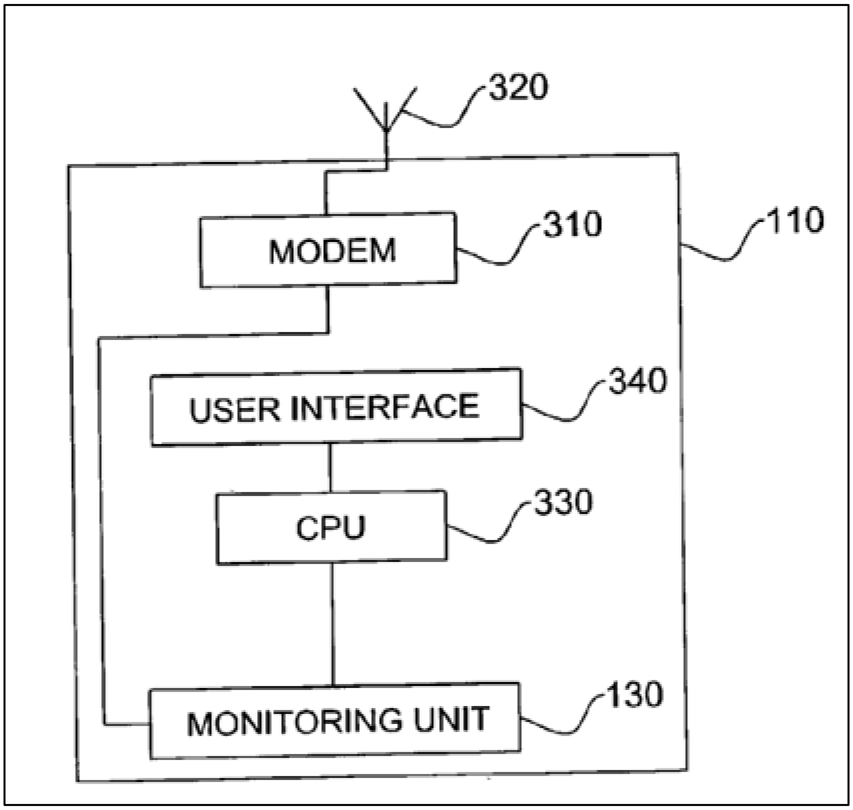
SAMSUNG-1007, FIG. 1.

This unit receives "reports on the data activity from the [device], rate[s] the data activity, and update[s] at least one allowance of the account based on a result of the rating." *Id.* The "rating of a voice event is typically based on rules related to the event (for example, the duration of the call, ..., etc.) and/or related to the account (for example, the number of free minutes per period, ..., etc.)." SAMSUNG-1007, [0002], Abstract; [0035]-[0037].

The monitoring unit sends data activity reports to the server utility, which rates "the data activity reported by the monitoring units." SAMSUNG-1007, [0042],

[0045]-[0047], [0062]. The "transmission may periodically be initiated by monitoring unit 130, e.g., automatically after passage of a predefined time." SAMSUNG-1007, [0062].

FIG. 3A shows Bittmann's monitoring unit coupled to the device's modem. SAMSUNG-1007, [0052], FIG. 3A. Bittmann explains that the "link between monitoring unit 130 and receiver/transmitter" of the device enables "transmit[ting] stored activity data, through the cellular communication infrastructure, to server utility 150, preferably as out-of-band traffic." SAMSUNG-1007, [0053]. Additionally, "the link is configured" "to cause all data received by the associated communication device" "to be intercepted by monitoring unit 130 prior to becoming available to" the device user. SAMSUNG-1007, [0053].



SAMSUNG-1007, FIG. 3A.

2. *Combination of Schmidt, De Beer, and Bittmann*

As explained in §III.A.3, SDD's mobile device includes a SEE and secure modem subsystem, and is configured to implement a vSIM service that provides the function of a conventional SIM. SAMSUNG-1003, ¶175.

Per DB, SDD connects to a "home" cellular network associated with a service provider through a contractual relationship. SAMSUNG-1006, [0030], [0035]; SAMSUNG-1003, ¶176. Given that SDD facilitates use of services provided over a cellular network using the vSIM service, SDD leverages DB teachings of storing and

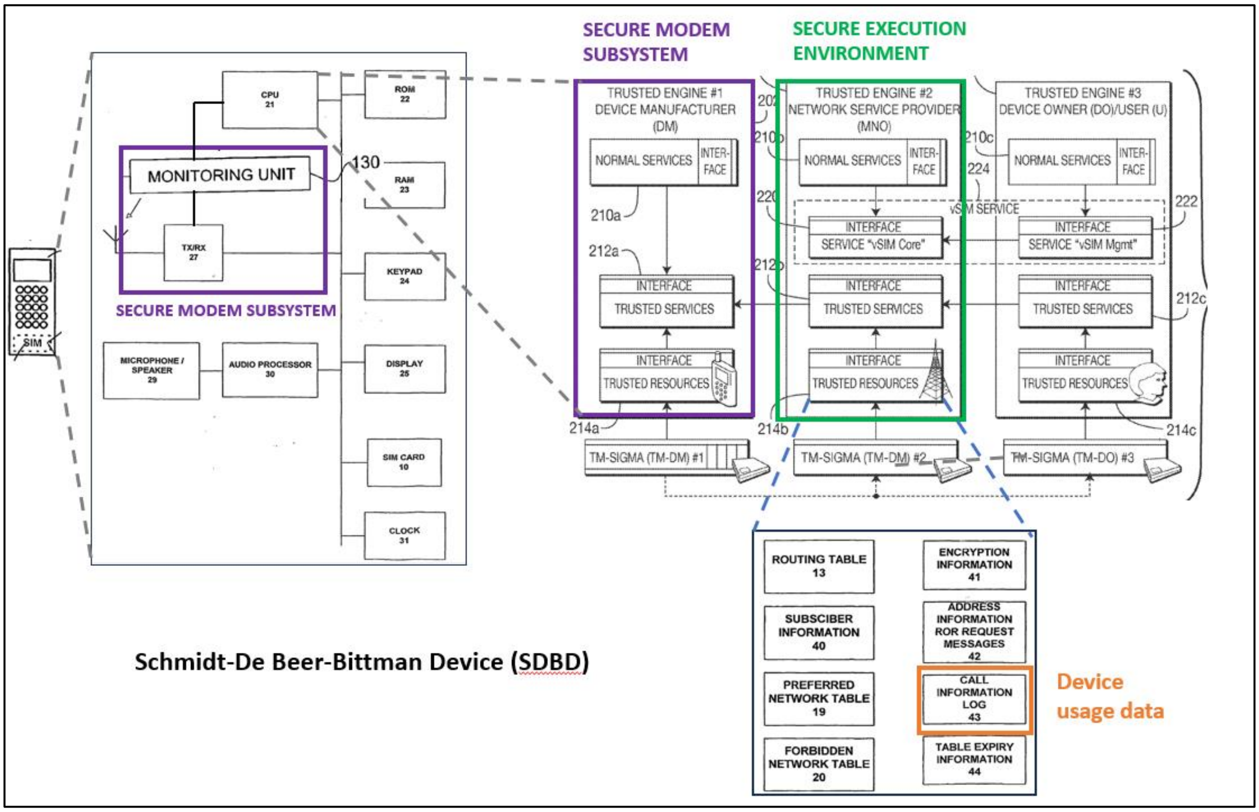
tracking data related to the use of these services. SAMSUNG-1003, ¶176. For example, DB's device uses a call log, which is stored on the SIM, "for storing the duration and call destination of calls." SAMSUNG-1006, [0090], [0049], FIG. 4. The device periodically communicates this log "to the control centre 14 by including call log information in the request message." SAMSUNG-1006, [0090], [0101]. The control centre uses the log "to verify billing information generated by networks within the generalised network 12 and by the local network." SAMSUNG-1006, [0090].

While DB explains that such data is captured and stored in a log, DB does not explicitly describe techniques for obtaining this log data. SAMSUNG-1003, ¶177.

A POSITA would have thus been motivated to look to references such as Bittmann, which describes a mobile device that includes a monitoring unit that monitors a device's network activity, provides reports to a server (similar to DB), and enforces service plan limits. §III.B.1; SAMSUNG-1003, ¶178. The resulting Schmidt-DB-Bittmann device (SDBD) includes the components of SDD, enhanced by Bittmann's monitoring unit, which monitors device usage and enforces service plan limits. SAMSUNG-1003, ¶178. The monitoring unit would be included in SDBD's secure modem subsystem, enabling it to "monitor[] data activity of communication device" and to "cause all data received by the associated communication device ... to be intercepted by monitoring unit 130 prior to becoming available to the

user of communication device," per Bittmann. SAMSUNG-1007, [0028], [0031], [0053]; SAMSUNG-1003, ¶178.

A POSITA would understand that by including the monitoring unit in the secure modem subsystem, the monitoring unit has efficient access to all data transferred via the device. SAMSUNG-1003, ¶¶178-179. Also in the context of SDD, which replaces the SIM card with a vSIM service, the call log data would be stored in SDD's secure memory partition. SAMSUNG-1006, [0049], FIG. 4; SAMSUNG-1003, ¶179.



SAMSUNG-1005, FIG. 2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified);

SAMSUNG-1007, FIG. 3A (modified).

In operation, to ensure compliance with the service plan, SDBD's monitoring unit monitors the device's inbound and outbound traffic and stores the data in SDD's secure storage/memory partition. SAMSUNG-1006, [0049], FIG. 4; SAMSUNG-1007, [0028], [0031], [0053]; SAMSUNG-1003, ¶180; *See* §III.A.3.

SDBD transmits data activity reports to a server, which rates "the data activity reported by the monitoring units." SAMSUNG-1007, [0042], [0062]; SAMSUNG-1003, ¶181. A POSITA would understand that Bittmann's server utility would execute on DB's control centre because both DB's control centre and Bittmann's server receive device usage data. SAMSUNG-1003, ¶181; SAMSUNG-1006, [0101]; SAMSUNG-1007, [0053].

A POSITA would have expected success in implementing a monitoring unit, per Bittmann, within SDD, which requires only routine programming knowledge well within a POSITA's skill. SAMSUNG-1003, ¶182. Indeed, this would have amounted to using a known technique to improve similar devices—a communication device configured to monitor device operation (e.g., SDD's call logging per DB, and Bittmann's monitoring)—in a similar way and combining prior art elements according to known methods to yield the predictable results described above. SAMSUNG-

1006, [0049], [0076], [0092], [0101]-[0102]; §III.A.3; SAMSUNG-1003, ¶182. Indeed, both SDD and Bittmann's device describe performing conventional monitoring and reporting monitored device activity. SAMSUNG-1006, [0049], [0076], [0092], [0101]-[0102]; §III.A.3; SAMSUNG-1003, ¶182.

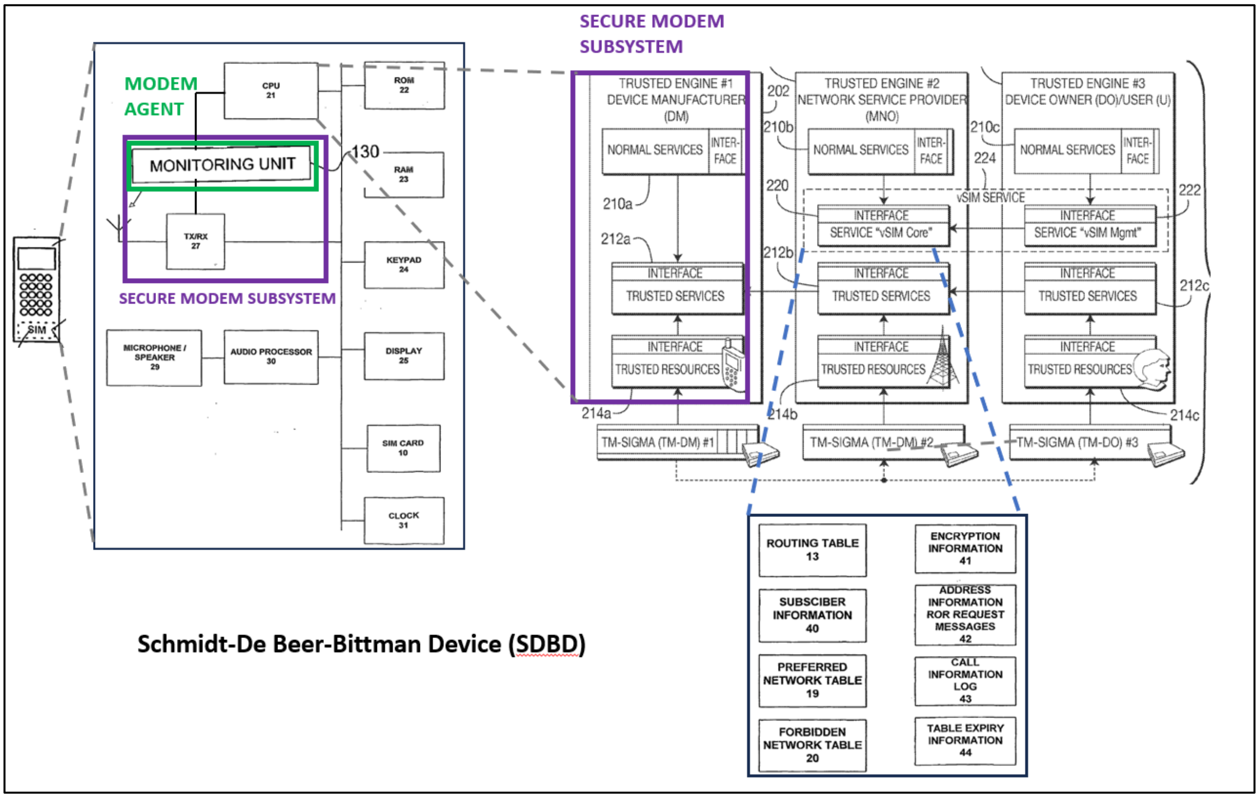
Finally, the elements of the resulting SDBD would each perform functions they performed prior to combination—SDD leverages an installed vSIM credential to connect to cellular networks, including while roaming, and Bittmann's monitoring unit monitors and reports device activity. §III.A.1-3; §III.B.1; SAMSUNG-1003, ¶183. Further, SDBD's monitoring unit transmits data using SDD's modem subsystem much like Bittmann's monitoring unit transmits data over a modem. SAMSUNG-1007, [0052]-[0053], [0055], FIG. 3A; §III.A.3; SAMSUNG-1003, ¶183. A POSITA would have therefore expected success when combining Bittmann's teachings with SDD. SAMSUNG-1003, ¶183.

3. Analysis

[4]

SDBD's secure modem subsystem includes a modem agent (activity monitoring unit, per Bittmann), enabling SDBD to monitor "data transferred to and/or from device." §III.B.2; SAMSUNG-1007, [0031]; SAMSUNG-1003, ¶¶281-282. Per Bittmann, the "activity monitoring unit" "links between a CPU … and a network

interface," and "monitors data activity of [the] communication device." SAMSUNG-1007, [0028], [0052].



SAMSUNG-1005, FIG. 2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified);

SAMSUNG-1007, FIG. 3A (modified).

The secure modem subsystem, and therefore the monitoring unit (modem agent) is only accessible by the network service controller (control centre) through the first secure control channel (control channel between TSS-DM and control centre, per [1.3] above). SAMSUNG-1003, ¶282. For example, per Schmidt, TSS-DM "controls all internal and external communications." SAMSUNG-1005, [0032]. Therefore, the network service controller (control centre) accesses the modem agent

only through the secure control channel via TSS-DM. SAMSUNG-1003, ¶282. A POSITA would further understand or find obvious that the modem agent is accessible to the network service controller only through the first control channel. SAMSUNG-1003, ¶282. That's because, when the first control channel is active, that channel would be the only dedicated connection between the control centre and the secure modem subsystem. which includes the modem agent (monitoring unit). SAMSUNG-1003, ¶282. As described in [1.3] and [1.4], only one control channel is active at a time – that is, the first and second control channel differ based on time of occurrence. SAMSUNG-1022, 3; SAMSUNG-1003, ¶282.)

[5]

SDBD's modem agent (e.g., monitoring unit, per Bittmann) comprises a service measurement point for use of the service on the device. SAMSUNG-1007, [0028]-[0029], [0031]; SAMSUNG-1003, ¶¶283-286. Per Bittmann, the monitoring unit monitors the device's data activity. SAMSUNG-1007, [0031]. Bittmann further explains that "[e]xamples of the monitored data activity include inter-alia one or more of the following: web surfing, game-playing, emails, short message service (sms), ..., etc." SAMSUNG-1007, [0031].

A POSITA would understand or find obvious that SDBD's modem agent

would comprise the monitoring unit (service measurement point) because the modem agent would have efficient access to all cellular service data (and only cellular data) transferred to/from the device, thereby improving efficiency and conserving device resources. SAMSUNG-1003, ¶284.

Therefore, a POSITA would recognize or find obvious that the monitoring unit (modem agent) includes a service measurement point for services (such as voice and/or other data services, per [1.7] above) on the device (e.g., web surfing, SMS, voice). SAMSUNG-1007, [0031]; SAMSUNG-1003, ¶¶285-286; *see* [1.7] *supra*.

[6]

As described in [5], SDBD's modem agent (monitoring unit) monitors data activity of the device. SAMSUNG-1007, [0031]; §III.B.3.[5]; SAMSUNG-1003, ¶¶287-295. And, as explained in §III.A.3 and [1.6], data conventionally stored on a physical SIM would be stored in SDBD's secure memory partition. SAMSUNG-1003, ¶287. Therefore, in SDBD, a POSITA would understand or find obvious that the monitored data, which is also conventionally stored on the SIM (per DB), would be stored in the dedicated vSIM protected storage in the form of a secure memory partition (which as explained above would only be accessible by the TSS-MNO). SAMSUNG-1005, [0030]; SAMSUNG-1006, [0049], FIG. 4; SAMSUNG-1003, ¶245, ¶287; *see* §III.A.3.d *supra*.

In SDBD, the monitored call log data would be communicated from the device

to the control centre. SAMSUNG-1003, ¶288. Per DB, the call log "is ***periodically communicated to the control centre***." SAMSUNG-1006, [0090]. Bittmann similarly explains that the monitoring unit reports device data activity to a server, which manages the account of the device, e.g., to limit data activity if an account's allowance is exceeded. SAMSUNG-1007, [0029], [0037], [0043], [0046]; SAMSUNG-1003, ¶288.

Additionally, a POSITA would understand or find obvious to implement SDBD's system so that the monitored call log data is communicated from the TSS-MNO to the monitoring agent, and then from the monitoring agent to the control centre. SAMSUNG-1003, ¶289. As explained above, in SBDB, the call log stored in SDBD's secure memory partition is only accessible via the TSS-MNO. SAMSUNG-1005, [0028], FIG 2; SAMSUNG-1003, ¶289. Additionally, per Schmidt, TSS-MNO is responsible for "[a]ll subscription-dependent and subscriber-related network provider services," which would include provision of call log data (conventionally stored on a SIM, per De Beer) to the network controller, e.g., for billing or other associated functions related to use of network services. SAMSUNG-1005, [0033]; SAMSUNG-1006, [0049]; SAMSUNG-1003, ¶289.

Given these disclosures, a POSITA would recognize or find obvious that SDBD's system would be implemented so that either (1) the monitoring unit requests the call log data from the TSS-MNO, which then communicates this requested data

to the monitoring unit, or (2) the TSS-MNO communicates this data to the monitoring unit without being prompted to do so. SAMSUNG-1003, ¶290. Either would be straightforward to implement and would be a predictable solution to facilitate providing—which is only accessible by TSS-MNO—to the network service controller, via the monitoring unit in the secure modem subsystem. SAMSUNG-1003, ¶¶290-291.

Subsequently, per DB and Bittmann, this monitored call log would be communicated from the monitoring unit (i.e., modem agent), via the secure modem subsystem's components, to the control centre (i.e., network service controller). SAMSUNG-1003, ¶292; *see, e.g.*, SAMSUNG-1007, [0042] (sending "data activity reports ***from monitoring units***," which are part of SDBD's secure modem subsystem), [0053] ("[t]he link between monitoring unit 130 and receiver/transmitter" allows "unit 130 to transmit stored activity data"); SAMSUNG-1006, [0090].

Additionally, in SDBD, the data activity report would be communicated by the monitoring unit through the first secure control channel. SAMSUNG-1003, ¶293. Per Bittmann, "[t]he link between monitoring unit 130 and receiver/transmitter" allows "unit 130 to transmit stored activity data, through the cellular communication infrastructure, to server utility 150, preferably as ***out-of-band traffic***." SAMSUNG-1007, [0053]. A POSITA would understand that control channels, including SDCCH, transmits traffic out-of-band. §IIIA.3.[1.3]; SAMSUNG-1003, ¶293,

§VII.C.

Moreover, because SDBD would have already established a first control channel (e.g., SDCCH) between the device and the control centre, a POSITA would understand or find obvious that, when transmitting stored activity data out-of-band to the control centre, SDBD would use the same first control channel. *See* analysis for [1.3] *supra;* SAMSUNG-1003, ¶294. That's because that would have been conventional and straightforward, and would improve efficiency and conserve resources. *Id.*

For these reasons, the TSS-MNO of SDBD's SEE communicates a first report of the use of the service to the modem agent (monitoring unit in the secure modem subsystem), which then would communicate the report to the network service controller (control centre) through the first secure control channel. SAMSUNG-1003, ¶295.

[7]

As described in [6], SDBD would periodically communicate monitored call logs/usage reports (i.e., the monitored use of the service) from the SEE (including TSS-MNO) through the secure modem subsystem (including the monitoring unit and TX/RX) to the control centre (network services controller). *See* [6], *supra.*

Moreover, as explained in [6], at a first time, SDBD would communicate a

first report over the first secure control channel. At a later time (e.g., on the next day), there would be a second secure control channel with the control centre, and SDBD would communicate a second report of monitored use through that second secure control channel. SAMSUNG-1003, ¶297. Specifically, as explained in [1.4], the second control channel is established at a later time from the first secure control channel, such as the next day. Therefore, when SDBD communicates the report (the "call log ... is ***periodically communicated to the control centre***"), a POSITA would understand or find obvious that the report is transmitted over the second secure control channel, which is the only control channel available with the control centre at that time. *See* [1.4]; SAMSUNG-1006, [0090]; SAMSUNG-1003, ¶297.

Therefore, in SDBD, the SEE (TSS-MNO/TM-SIGMA) separately communicates a second report (at a later time than the first report) of the monitored use of the service (via the secure modem subsystem) to the network service controller and using the second secure control channel (the only channel available at that later time). SAMSUNG-1003, ¶¶296-298.

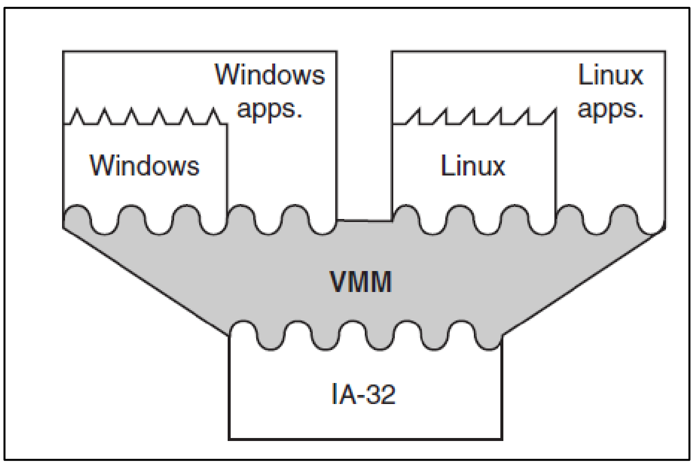
C. GROUND 1C – Schmidt-De Beer-Smith Renders Obvious Claims 10-12

1. Smith

Smith describes various types of virtual machines (VMs), including system VMs, that "provide a complete system environment in which many processes[] can coexist." SAMSUNG-1008, 25; SAMSUNG-1012, 72. Per Smith, VMs "provide

a secure way of partitioning major software systems that run concurrently on the same hardware platform" such that "[s]oftware running" in one VM environment "is isolated from software running on other guest systems." SAMSUNG-1008, 18, 26, 29; SAMSUNG-1012, 72, 506-507; SAMSUNG-1003, ¶¶184-186.

Smith further explains that VMs enable "support [of] different operating systems simultaneously." SAMSUNG-1008, 26; SAMSUNG-1012, 72. Smith provides one example (below) showing, on a single device, a Windows VM running Windows applications and a Linux VM running Linux applications. *Id.*



SAMSUNG-1008/SAMSUNG-1012, FIG. 1.11

2. Combination of Schmidt, DB, Smith

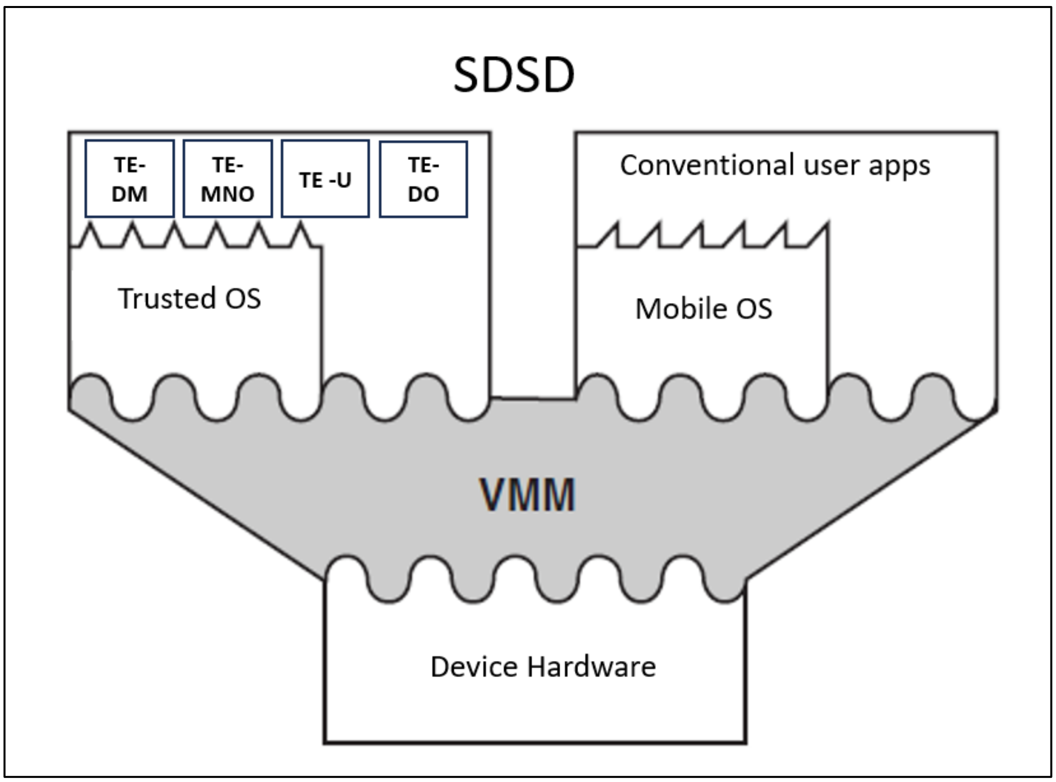
As explained in §III.A, Schmidt provides a wireless end-user/mobile device in which a "MTP operates a trusted operating system" (OS). SAMSUNG-1005, [0036], [0096]. A POSITA understands or finds obvious that mobile devices addi-

tionally run user applications, e.g., e-mail, browsers, etc., which would run in a conventional OS. SAMSUNG-1003, ¶187; SAMSUNG-1006, [0083]; SAMSUNG-1062, [0092]. Thus, while SDD includes a trusted OS (per Schmidt) and user applications (operating in a separate, conventional OS), Schmidt does not expressly describe how such applications and OSs operate simultaneously and are isolated from each other. SAMSUNG-1003, ¶187.

A POSITA would have looked to references, such as Smith, that provide implementation details and explain that VMs achieve Schmidt's desired isolation of secure environments from generalized environments. SAMSUNG-1003, ¶188. Per Smith, VMs enable "support [for] different operating systems simultaneously," which thus enables concurrent execution of Schmidt's TSSs and other applications on SDD. SAMSUNG-1008, 26; SAMSUNG-1012, 72; SAMSUNG-1003, ¶188. Further, Smith explains that VMs "provide a secure way of partitioning major software systems" to isolate software therein. SAMSUNG-1008, 26, SAMSUNG-1012, 72; SAMSUNG-1003, ¶188; §III.C.1. Smith also explains that "[r]unning each application in its own virtual machine increases the robustness of the system," since erratic behavior on a VM is "less likely to affect the operation" of applications running on a different VM. SAMSUNG-1008, 29; SAMSUNG-1012, 506-507. Thus, to increase SDD's robustness, a POSITA would have been motivated to implement

SDD's TSSs to run in a VM separate from an environment running the user application (e.g., which may be implemented in another VM). SAMSUNG-1003, ¶188.

The resulting Schmidt-DB-Smith device (SDSD) includes, per Smith, a VM Monitor (VMM), which is virtualizing software that provides two VMs, one hosting Schmidt's trusted OS and trusted engines (TSS-DM, TSS-MNO, etc.), and another hosting a second OS running conventional applications, as illustrated below. SAMSUNG-1003, ¶189; SAMSUNG-1008, 24; SAMSUNG-1012, 72-73.



SAMSUNG-1008/SAMSUNG-1012, FIG. 1.11(modified); SAMSUNG-1003, ¶189.[5]

---

[5] SDSD further includes components, omitted from this figure for clarity, such as TX/RX, multiple TM-SIGMAs, etc. SAMSUNG-1003, ¶189 n.17.

As shown, because the MTP-related software runs in a VM apart from a user-application VM, erratic behavior of user applications is "less likely to affect the operation of" the MTP applications (executing on a different VM), thereby improving device stability. SAMSUNG-1008, 29; SAMSUNG-1012, 506-507; SAMSUNG-1003, ¶190.

Schmidt also explains that the system must "prevent loss and escape of security-sensitive data," and ensure that necessary services are "available and functional." SAMSUNG-1005, [0040]. Since Smith teaches that VMs isolate software running in a VM and "increase[] the robustness of the system," a POSITA would have further been motivated to run Schmidt's MTP in a system VM, isolating the MTP, "prevent[ing] loss and escape of security-sensitive data and ensur[ing] that all necessary services are available and functional," even if other device applications, running outside the MTP malfunction. SAMSUNG-1005, [0040]; SAMSUNG-1008, 24, 26, 29; SAMSUNG-1012, 72-73, 506-507; SAMSUNG-1003, ¶191.

A POSITA would have expected success in implementing an MTP in a VM, because this would have required routine programming knowledge well-within a POSITA's skill. SAMSUNG-1003, ¶192. Indeed, this would have amounted to using a known technique (VMs) to improve operation of a known device (SDD) to achieve predictable results (running software in a VM). SAMSUNG-1003, ¶192.

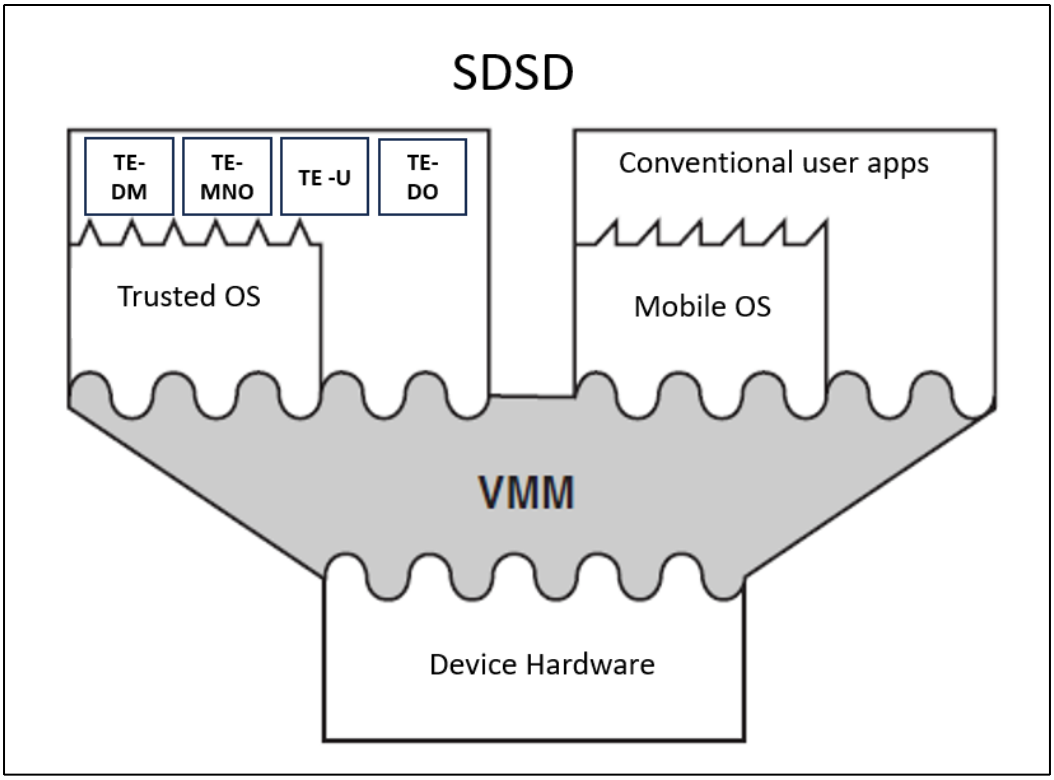
Finally, the elements of SDSD each perform functions they performed prior

to combination—Smith's environment provides VMs that isolate SDD's trusted OS from end-user applications, SDD trusted OS downloads and manages the vSIM, and the device operates while roaming per DB. SAMSUNG-1003, ¶193. A POSITA would have therefore expected success when combining Smith's teachings with SDD. SAMSUNG-1003, ¶193.

3. Analysis

[12]

In SDSD, the MTP, which includes the SEE (TSS-MNO/TM-SIGMA), runs in a system VM (*see supra* §III.A.3, §III.A.4.[1.4]; §III.C.2), which executes on a device processor. SAMSUNG-1003, ¶303; SAMSUNG-1008, 25-26, FIG. 1.11 (system VM runs on IA-32 hardware platform that includes a processor); SAMSUNG-1012, 72, FIG. 1.11; SAMSUNG-1003, ¶¶302-304 (Schmidt's device including a processor that runs the device software and OS).



SAMSUNG-1008/SAMSUNG-1012, FIG. 1.11(modified); SAMSUNG-1003, ¶304.

[10]

Per Smith, SDSD's VM "is implemented as a combination of a real machine and virtualizing software," the latter "partition[ing] a single large hard disk into" multiple "smaller virtual disks." SAMSUNG-1008, 14, 18, 34; SAMSUNG-1012, 55, 63, 549. Further, TSS-MNO includes trusted resources, including trusted storage, which is a hardware partition (created by the VMM) of SDSD's physical storage. SAMSUNG-1003, ¶299-300; SAMSUNG-1030, 28. §III.A.4.[1.6].

Thus, SDSD's SEE is implemented in part as a hardware partition (a trusted storage partition in TSS-MNO). SAMSUNG-1005, [0033]; SAMSUNG-1003, ¶300.

[11]

In SDSD, the MTP is implemented as a VM. SAMSUNG-1003, ¶301; *see* §III.C.1-2. A VM is a software partition because it "provide[s] a secure way of partitioning major software systems" running on a hardware platform. SAMSUNG-1008, 24; SAMSUNG-1012, 72-73; SAMSUNG-1003, ¶301.

IV. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. §325(d)

The references presented herein were not previously before the Office. *See generally*, SAMSUNG-1002. Thus, the Office has not considered these references or combinations presented in this Petition. Moreover, the same or substantially the same arguments were not previously presented to the Office. Indeed, there could be no overlap with the arguments made before the Office because the Examiner issued no prior art rejections during prosecution. *Id*.

Further, material error occurred during prosecution because Examiner failed to consider the above-presented grounds, and how they rendered obvious the Challenged Claims. Indeed, Petitioner has shown a reasonable likelihood that at least one of the Challenged Claims is unpatentable over the applied art on the current record. *Supra* §III; *Tokyo Ohka Kogyo Co., Ltd. v. Fujifilm Elec. Materials U.S.A., Inc.*, PGR2022-00010, Paper 9, 8-9 (PTAB June 6, 2022). Therefore, §325(d) discretionary denial is not warranted.

B. §314(a)

This Petition's merits are compelling, and the evidence presented herein is substantial, counseling against discretionary denial under *Fintiv*. SAMSUNG-1009 4-5. Moreover, the *Fintiv* factors counsel against denial.

Factor 1 is neutral because neither party has requested a stay in the copending litigation.

Factor 2 is neutral because the Court's trial date is speculative and subject to change. The Board will likely issue its Final Written Decision around July/August 2026, approximately 5-6 months after the currently-scheduled trial date (February 9, 2026). SAMSUNG-1011, 1. However, as the Board/Director have recognized, "scheduled trial dates are unreliable and often change." SAMSUNG-1009, 8.

Factor 3 favors institution because Petitioner has diligently filed this Petition months ahead of the one-year time bar, while the copending Litigation is in its early stages. Beyond exchanging preliminary infringement and invalidity contentions, the parties and the court have yet to expend significant resources on invalidity. SAMSUNG-1011. By the anticipated institution deadline in July/August 2025, the co-pending litigation will still be in early stages—fact and expert discovery will be on-going, and the *Markman* hearing will likely not have occurred. *Id.*

Factor 4 favors institution because Petitioner stipulates to not pursuing the IPR grounds in the co-pending litigation. SAMSUNG-1010. Thus, institution

serves "efficiency and integrity goals" by "not duplicating efforts" and "resolving materially different patentability issues." *Apple, Inc. v. SEVEN Networks, LLC*, IPR2020-00156, Paper 10, 19 (June 15, 2020); *Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019,-01393, Paper 24, 12 (June 16, 2020); *Google LLC v. Flypsi, Inc.*, IPR2023-00360, Paper 9, 36-39 (August 2, 2023).

Factor 5: Same parties are in the co-pending litigation.

Factor 6 favors institution because this Petition's merits are compelling, as described herein.

V. CONCLUSION

The Challenged Claims are unpatentable. Petitioner authorizes charge of fees to Deposit Account 06-1050.

VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(A)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Samsung") are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '429 Patent is the subject of civil action Headwater Research LLC v. Samsung Electronics Co., Ltd. et al 2-24-cv-00228 (EDTX), filed April 3, 2024. Petitioner is not aware of any disclaimers, reexamination certificates, or IPR petitions addressing the '429 Patent.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR39843-0185IP1@fr.com	Jeremy J. Monaldo, Reg. No. 58,680 Karan Jhurani, Reg. No. 71,777 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information

Please address all correspondence and service to the address listed above. Petitioner consents to electronic service by email at IPR39843-0185IP1@fr.com (referencing No. 39843-0185IP1 and cc'ing PTABInbound@fr.com).

Respectfully submitted,

Dated 01/28/2025

/Karan Jhurani/
W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Karan Jhurani, Reg. No. 71,777
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2025-00482)

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,988 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated 01/28/2025

/Karan Jhurani/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Karan Jhurani, Reg. No. 71,777
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on January 28, 2025, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

/Diana Bradley/

Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
bradley@fr.com